FOM Fachhochschule für Ökonomie und Management
Neuss

Berufsbegleitender Studiengang zur Erlangung des Grads
Bachelor of Information Technology Engineering (B.Sc.)

Firewalls für kleine und mittelständische Unternehmen auf Basis des OpenSource-Projektes IPCop

Autor: Stefan Kox
Matrikelnr.: 119532
Betreuer: Prof. Dr.-Ing. Torsten Finke
Ort, Datum: Nettetal, 14.02.2008

Vorwort

Sicherlich gibt es zum Thema *Firewalls* bereits zahlreiche Lösungen und Untersuchungen und es wurde auch schon in vielen Varianten bearbeitet. Jede Arbeit hat jedoch, für sich selber gesehen, seine Daseinsberechtigung. So auch diese. Meine Intention bei der Erstellung dieser Arbeit liegt zum einen in der Tatsache, dass es bis zum Zeitpunkt der Erstellung dieser Arbeit keinerlei Literatur in Form eines deutschen Fachbuchs über die Firewall IPCop gab, zum anderen in der Definition der Zielgruppe. Erst mit Fertigstellung dieser Arbeit erscheint ein Buch über die verwendete Firewall IPCop. Daher können auch keine Informationen aus diesem Buch mit in diese Arbeit einfließen.

Trotz einer recht großen Community im Internet und zahlreicher Seiten mit unzähligen Informationen über den IPCop fehlte es bislang immer noch an einem zentralen Werk in dem die wichtigsten Themen gesammelt sind. Die Seiten im Internet beschäftigen sich meist nur mit einem speziellen Thema zur Firewall selbst, beziehungsweise behandeln in erster Linie das dort angebotene AddOn. Weiterführende Informationen sind dort in der Regel nicht erhältlich. Die wohl wichtigsten Anlaufpunkte im Netz sind das deutsche Forum zum IPCop sowie die englischsprachige Projektseite.

Nach Fertigstellung dieser Arbeit beabsichtige ich die Arbeit weiter auszubauen und fortzuführen. Dann möchte ich auf tieferliegende Details eingehen, die innerhalb dieser Arbeit nicht untersucht werden können. Die längerfristige Zielsetzung besteht darin, ein deutsches Fachbuch zum IPCop zu schreiben, welches primär die Absicherung kleiner und mittlerer Netzwerke beschreibt.

Die Zielgruppe der vorliegenden Arbeit sind jedoch, wie im Titel bereits definiert, kleine und mittelständische Unternehmen. Die Größe der in Betracht kommenden Unternehmen sollte bei weniger als 50 Mitarbeitern (Benutzer/Clients) liegen, obwohl in weiteren Ausbaustufen auch eine größere Nutzergruppe möglich ist.

Bei der genannten Zielgruppe liegt allerdings in vielen Fällen das Hauptziel in der Umsetzung von IT-relevanten Themen zu einem geringen Preis. Oft besteht die IT-Abteilung eines solchen Unternehmens aus einem Team von einem bis drei Mitarbeitern (inkl. vorhandener Auszubildenden), die sich mit allen EDV-technischen Themen des Unternehmens beschäftigen. Dazu gehört unter anderem ein Benutzermanagement, Sicherungsmanagement, Installation und Einrichtung der Arbeitsplatzrechner und Server, Wartung und Fehlerbehebung der IT-Infrastruktur sowie die Pflege der hauseigenen Webseiten. In vielen Fällen kommt noch der umfangreiche Bereich der Telekommunikation dazu.

Die Erfahrung meiner mehr als zehn-jährigen Berufslaufbahn zeigt jedoch, dass die Geschäftsleitung, wenn auch zögerlich bereit ist in Sicherheit zu investieren, jedoch nur in beschränktem Maß. Das Management unterliegt oft der Fehleinschätzung, dass das Unternehmen nicht gefährdet sei. Oder noch naiver, dem Management ist bekannt, dass das Unternehmen angegriffen werden kann, dadurch aber kein Schaden entstehen würde. Diese Art der Gefährdungseinschätzung führt dazu, dass es einen ungeschützten Zugang zum Internet gibt. Wenn dann auch noch Serverdienste wie E-Mail, Datenbanken oder Webseiten angeboten werden ohne diese zu schützen, ist es nicht mehr eine Frage, ob das Unternehmen angegriffen wird, sondern wann und wie hoch der Schaden wird. In der Realität sieht es nach eigener Erfahrung und zum Zeitpunkt der Erstellung dieser Arbeit so aus, dass ein nicht geschützter Zugang zum Internet innerhalb der ersten 30 Minuten bereits angegriffen wird.

Schon allein aus diesem Grund betrachte ich es als notwendig, dieser Zielgruppe ein geeignetes Werk(-zeug) zur Verfügung zu stellen, um aufzuklären womit ein einzelner Rechner, ein Netzwerk und somit das gesamte Unternehmen geschützt werden kann.

Die in dieser Arbeit dokumentierte Software IPCop stellt ein solches Werkzeug dar. Da IPCop als OpenSource-Projekt angeboten wird, ist dieses auch kostenneutral. Lediglich die Anschaffung der Hardware (in der Regel bereits vorhanden), die Einrichtung und der Betrieb stellen noch einen Kostenfaktor dar.

Inhaltsverzeichnis

Vorwort **II**

Abbildungsverzeichnis **VII**

Tabellenverzeichnis **IX**

1 Einleitung **1**

2 Firewall Grundlagen **3**
2.1 Angreifer 4
2.2 Angriffsmöglichkeiten 5
2.2.1 Denial of Service (DoS) 5
2.2.2 Spoofing 6
2.2.3 Hijacking 8
2.2.4 SQL-Injection 8
2.3 Schutzmöglichkeiten durch Firewall Architektur 8
2.3.1 Paketfilter 9
2.3.2 Proxy 9
2.3.3 NAT - Network Address Translation 10
2.4 Einsatzszenarien und Konzepte 11

3 IPCop **14**
3.1 Netzwerk 15
3.2 Netzwerkkonfiguration 17
3.3 Funktionsumfang 18
3.4 Installation 18
3.4.1 Hardwarevoraussetzungen 19
3.4.2 Installationsvorgang 20
3.4.3 IPCop in virtuellen Maschinen 22

4 Konfiguration und Einrichtung der Basismodule 24
4.1 Allgemeine Einstellungen . . . 24
4.1.1 Updates . . . 25
4.1.2 Passwörter . . . 25
4.1.3 SSH-Zugriff . . . 26
4.1.4 Einstellungen der Benutzeroberfläche . . . 26
4.1.5 Datensicherung . . . 27
4.1.6 Herunterfahren . . . 27
4.1.7 Dank an... . . . 27
4.2 Statusmeldungen . . . 27
4.2.1 Systemstatus und Diagramme . . . 28
4.2.2 Verbindungen . . . 29
4.3 Netzwerk . . . 29
4.4 Dienste . . . 31
4.4.1 WebProxy . . . 31
4.4.2 DNS-Server . . . 32
4.4.3 DHCP-Dienst . . . 32
4.4.4 Zeitserver . . . 33
4.4.5 Dynamisches-DNS . . . 33
4.4.6 Intrusion Detection . . . 34
4.4.7 Traffic Shaping . . . 35
4.5 Firewall . . . 35
4.5.1 Port-Forwarding . . . 35
4.5.2 Externer Zugang . . . 36
4.5.3 DMZ-Schlupflöcher . . . 36
4.5.4 Firewall Optionen . . . 36
4.6 VPN . . . 37

5 Weitere Funktionen und Dienste - AddOns 39
5.1 Quality of Service . . . 41
5.2 BlockOutTraffic . . . 43
5.3 Advanced Proxy . . . 46
5.3.1 Update Accelerator . . . 51
5.3.2 Calamaris . . . 52
5.4 URL filter . . . 54

5.5 Copfilter 56
5.5.1 Quarantäne 58
5.5.2 Monit 58
5.5.3 P3Scan 59
5.5.4 ProxSMTP 60
5.5.5 HAVP 61
5.5.6 Privoxy 61
5.5.7 frox 61
5.5.8 SpamAssassin 62
5.5.9 Virenscanner 63
5.5.10 ClamAV 64
5.5.11 F-Prot und AVG 64
5.5.12 Tests und Logs 65
5.6 High Availability - Ucarp 65
5.7 Webalizer 67
5.8 LineTest 68
5.9 GUI-Ports 69
5.10 UPS 70
5.11 SystemInfo 72
5.12 SnortALog 73
5.13 FireWall Logs 74
5.14 RootkitHunter 75
5.15 Coptime 76

6 Wartung und Pflege 78
6.1 Updates 78
6.2 Logauswertung 80
6.3 Stabilität 81
6.4 Hilfestellung und Ressourcen 83

7 Zusammenfassung 86

Glossar I

Literaturverzeichnis IV

Abbildungsverzeichnis

1.1 Die IPCop Logos 1

2.1 Schematische Darstellung eines Paketfilters 9
2.2 Schematische Darstellung eines Proxies 10
2.3 Schematische Darstellung eines Screened Host 12
2.4 Schematische Darstellung eines Screened Subnet 12

3.1 Netzwerk Anbindung über ein Modem 17
3.2 Netzwerk Anbindung über einen Router 18
3.3 Netzwerk mit einer DMZ 18
3.4 Screenshots der Installations- und Konfigurationsdialoge 21

4.1 Screenshot des IPCop-Startbildschirm 25
4.2 Screenshot der SSH-Verbindung mit Putty 26
4.3 Screenshot der IPCop-Statusinformation 28
4.4 Screenshot des IPCop-Diagramms der grünen Schnittstelle 29
4.5 Screenshot der IPCop-Verbindungsverfolgung 30

5.1 QoS Funktionsweise 42
5.2 Screenshot BOT Regeln in einem IPCop 43
5.3 Screenshot Konfigurationsmaske Advanced Proxy 47
5.4 Screenshot Konfigurationsmaske Calamaris 53
5.5 Screenshot Startseite des Copfilter AddOns 57
5.6 Screenshot Quarantäne des Copfilters 59
5.7 Schema des High Availability AddOns - Ucarp 66
5.8 Screenshot Bericht des Webalizer AddOns 68
5.9 Screenshot Konfigurationsmaske GUI-Ports 70
5.10 Screenshot UPS Zusammenfassung 71
5.11 Screenshot Bericht des AddOns SnortALog 73

5.12 Screenshot Bericht des AddOns Firewall Logs 75
5.13 Screenshot Konfigurationsmaske Coptime 77

6.1 CopTime User - Jahresansicht 82
6.2 Uptimesumme - Jahresansicht 82
6.3 Durchschnittliche Uptime - Jahresansicht 82

Tabellenverzeichnis

3.1 Schnittstellen im IPCop 16
3.2 Regelwerk im IPCop 16

5.1 Übersicht AddOns 40
5.2 Übersicht Klassen 42
5.3 Speicher/Cache Ersetzungsrichtlinie 49

6.1 Übersicht Foren Bereiche 84

7.1 Übersicht Addons - Funktionsumfang/Nutzen 88

1 Einleitung

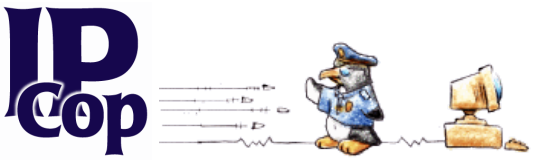


Abbildung 1.1: Die IPCop Logos

Die vorliegende Arbeit beschäftigt sich mit dem Thema der Firewall, speziell mit der frei verfügbaren Linux-Distribution IPCop. IPCop ist eine Software, die auf einem Rechner installiert wird und im wesentlichen Routing-Dienste und einen Paket-Filter zur Verfügung stellt. Aktuell ist zum Zeitpunkt der Erstellung dieser Arbeit die Version 1.4.18. welche auch als Grundlage bei der Erstellung dieser Arbeit herangezogen wird. Abbildung 1.1 zeigt die Logos des IPCops. Sie dienen als Erkennungsmerkmal.

Die Arbeit richtet sich primär an in EDV-technischen Positionen arbeitende Personen, die sich mit der Planung, Einrichtung und Betreuung eines Netzwerks beschäftigen. Grundlegende Kenntnisse über die Funktion von Netzwerken und Technologien werden für das Verständnis beim Lesen vorausgesetzt. Ebenso empfiehlt es sich, dass der Leser ein Basiswissen im Umgang mit allgemeiner PC-Hardware besitzt. Sekundär ist aber auch jede private Person angesprochen, die den entsprechenden Kenntnisstand besitzt, um im privaten Umfeld ein sicheres Netzwerk unter Verwendung des IPCops einzurichten.

In größeren Netzwerken (als im Titel dieser Arbeit angegeben), wie etwa mit unterschiedlichen Netzwerksegmenten die untereinander auf unterschiedlicher Art und Weise miteinander kommunizieren wird der IPCop eher nicht mehr eingesetzt. Jedoch kann in dezentralen Netzwerken der IPCop als Gateway zur Verwendung kommen um diese Netzwerke untereinander zu verbinden. Die Eignung des IPCops in unterschiedlichen Netzwerken ist dabei ein weiterer Aspekt dieser Arbeit.

Zur übersichtlichen Trennung zwischen Text und Befehlen/Kommandos/Rechnereingaben, wurden solche in *kursiver Form* abgesetzt.

Vorgehensweise: Begonnen wird mit einer kurz gehaltenen Einführung in die Grundlagen der Arbeitsweise von Firewalls. Wichtige Begriffe werden vorgestellt und es wird auf die Unterschiede verschiedener Firewall-Architekturen und Technologien eingegangen (Kapitel 2). Dabei wird auch auf Angriffs- und Schutzmöglichkeiten eingegangen. Danach wird der IPCop vorgestellt (Kapitel 3).

Ein weiterer Punkt stellt die Kostensituation dar. Dazu wird unter anderem ermittelt, welche Hardware-Anforderungen sich ergeben und welchen Zeitaufwand die Einrichtung und anschließende Wartung der Software erfordert.

Im nächsten Abschnitt (Kapitel 4) wird die Installation und Konfiguration ausführlich erläutert. Dabei wird auch auf weitere Aufgaben der Software und Dienste wie Proxyserver, DHCP-Server, Zeitserver, Dynamische DNS Dienste, TrafficShaping, Intrusion Detection und VPN eingegangen. Zusätzlich können durch weitere frei verfügbare AddOns weitere Funktionalitäten der Software hinzugefügt werden. Einige der AddOns wie etwa Spamfilter, Virusfilter und Erweiterung des Proxys sind dabei Teil dieser Arbeit und werden auf Ihren Nutzen und Zweck untersucht.

Nach der Konfiguration werden weitere AddOns vorgestellt, deren Sinn und Zweck, sowie die Vor- und Nachteile dieser im nächsten Abschnitt beschrieben. Unter anderem wird hier über den allgemeinen Einsatz und die Notwendigkeit der diversen AddOns gesprochen (Kapitel 5).

Schließlich gibt es einen Abschnitt in dem Erfahrungswerte zur Stabilität und Wartbarkeit des Systems beschrieben sind. Alle vorgestellten Funktionen wurden dazu installiert und einer ausgiebigen Prüfung unterzogen. Die Ergebnisse finden sich zu den einzelnen Funktionen in den einzelnen Abschnitten und im Gesamten im letzten Abschnitt wieder (Kapitel 6).

Der Leser wird letztlich eine Dokumentation darüber erhalten mit welchen Mitteln er ein stabiles System zur Sicherung des Netzwerkes errichten kann. Dazu werden ihm Empfehlungen zur Installation, Konfiguration und Betrieb zur Verfügung gestellt. Er erhält Informationen über geeignete Maßnahmen zur SPAM- und Viren Bekämpfung und er bekommt darüber hinaus Informationen zur quantitativen und qualitativen Steuerung des Netzwerks via TrafficShaping/QoS und Proxyserver.

2 Firewall Grundlagen

Die Notwendigkeit für den Einsatz von Firewalls wurde ursprünglich, noch bevor das World Wide Web [4] 1989 von Tim Berners-Lee [36] entwickelt wurde, nicht mit dem Ziel begründet Netzwerke vor Angriffen durch Hacker zu schützen.

Aus den Ideen einiger Notizen von J.C.R. Licklider am MIT (Massachusetts Institute of Technology) und einer ersten frühen Arbeit Leonard Kleinrock's über packetvermittelnde Netzwerke entstand 1965 das erste WAN (Wide-Area-Network). Lawrence G. Roberts vernetzte zusammen mit Thomas Merill den TX-2 der Lincoln Labs, Massachusetts, mit dem Q-32 des SDC-California[52, Kapitel 1.1].

Roberts ging 1966 zur DARPA (Defense Advanced Research Projects Agency) von der das Projekt zur Entwicklung einer Vernetzung der Hochschulen finanziert wurde. Es entstand das ARPANET welches zu Beginn vier Forschungseinrichtungen untereinander vernetzte:

- Stanford Research Institute
- University of Utah
- University of California, Los Angeles
- University of California, Santa Barbara.

Es begann nun die Definition des ersten Protokolls für Netzwerke, dem Network Control Protocol (NCP) auf Basis dessen die erste Netzwerkanwendung entwickelt wurde, die E-Mail. Mit wachsender Größe des Netzwerks wuchs auch die Anzahl der Probleme und die Schwächen des Protokolls machten sich bemerkbar. Zum Beginn des Jahres 1983 wurde das Advanced Research Projects Agency Network (ARPANET) auf das heute noch bekannte Protokoll Transport Control Protocoll/Internet Protocol (TCP/IP) umgestellt.

Im Laufe der Zeit wurden nach und nach weitere Netzwerke aufgebaut, in denen jeder jedem vertraute. Maßnahmen zur Sicherheit wurden nur gegenüber technischen Schwierigkeiten implementiert, um die Qualität der Daten während der Übertragung zu gewährleisten. Bis zum

Auftreten des ersten Computerwurms, der von Robert Tappan Morris[35] 1988 entwickelt wurde, und zu dieser Zeit rd. 10% (damals ca. 6.000 Rechner) des Internets lahmlegte[52, Kapitel 1.2], existierten immer noch keine Firewalls. Es wurden lediglich Router zur Abschottung eines Netzwerks von anderen eingesetzt.

Die ersten Firewalls wurden erst kurz nach Auftreten des Morris Wurms relativ zeitgleich von AT&T und DEC entwickelt, die auf den Funktionalitäten von Proxies, dem Zwischenspeichern und Auswerten von Inhalten, basierten. Dies ist auch bis heute noch für gewisse Protokolle notwendig und sinnvoll um gegen SPAM und Viren ein Netzwerk zu schützen. Weiterhin enthält eine Firewall heute zusätzlich noch einen Paketfilter, der den Datenversand anhand ihres Typs und Status erkennt und entsprechend einem Regelwerk weiterverarbeitet[52, Kapitel 1.3].

2.1 Angreifer

Beim Einsatz einer Firewall stellt sich grundlegend die Frage, wer greift das Netzwerk an. Anderes formuliert, wer hat aus welchem Grund ein Interesse daran in ein Netzwerk einzudringen. Die Antwort klassifiziert sich in verschiedene Gruppen mit unterschiedlichem Anreiz und schwankendem Potential des Angriffs und ist in folgender Auflistung dargestellt[52, Kapitel 4].

- Skripptkiddies und Hacker
- Insider und Konkurrenz
- Spionage und Terroristen/organisierte Kriminalität

Von allen Gruppen gehen Gefahren aus. Das Gefahrenpotential steigt jedoch von Gruppe zu Gruppe und auch der Anreiz ändert sich. Skriptkiddies können aufgrund mangelnden Knowhows nur einen durch einen Hacker entwickelten Exploit, also der Ausnutzung einer bereits bekannten Schwachstelle, einsetzen. Beide Gruppen werden jedoch von Neugierde und Selbstbestätigung angetrieben und unterliegen eventuell sogar einem Messie-Syndrom, da es vielen nur um das Sammeln beliebiger Daten geht. Wobei der Hacker durchaus auch gegen Bezahlung Netzwerke angreift.

Der zweite Punkt, Insider und Konkurrenz stellt ebenso eine nicht zu unterschätzende Gefahrenquelle dar. Trotz mangelndem technischem Know-how kann der Insider aufgrund eines Racheakts nach seiner Kündigung in einem Unternehmen durchaus eine Gefahr darstellen.

Dem vertrauten und noch beschäftigtem Mitarbeiter wurden unter Umständen Zugänge zu unternehmenskritischen Punkten mitgeteilt. Diese können ein VPN-Zugang, Passwörter oder Dokumente auf Datenträgern sein. Werden diese Daten nach dem Ausscheiden aus dem Unternehmen nicht geändert, steht dem entlassenen Mitarbeiter Tür und Tor offen. Sollte dieser nun auch noch in einem Unternehmen beschäftigt werden, das sich in Konkurrenz zum vorherigen befindet, steht dem Datenklau nichts mehr im Weg. Aber auch ein Konkurrenzunternehmen ohne Insider kann einem Unternehmen Schaden zufügen, indem es einen Hacker zur Industriespionage anstiftet[52, Kapitel 4.2].

Somit ergibt sich auch der letzte Punkt, die Spionage durch Terroristen und organisierte Kriminalität. In Zeiten von Krieg (auch der kalte Krieg) und dem heute allgegenwärtigem Terrorismus ist es für beide Parteien unerlässlich an Informationen des Gegners zu gelangen, um diesem einen Schritt voraus zu sein. Eine staatlich gewollte Ausnahme stellt hier sicherlich der so genannte Bundestrojaner dar. Dieser soll zur Bekämpfung der Kriminalität ebenfalls zur Datenspionage eingesetzt werden. Von ihm geht ebenfalls eine nicht zu unterschätzende Gefahr aus, da dieser etwa durch einen begabten Hacker manipuliert und für illegale Aktivitäten ausgenutzt werden könnte.

2.2 Angriffsmöglichkeiten

Wie bereits eingangs erläutert, liegt die Angriffsmöglichkeit auf ein Netzwerk in den Schwachstellen der jeweiligen verwendeten Technologie. Durch den stufenweisen Ausbau von Beginn an und der Implementierung weiterer benötigter Funktionen, den daraus resultierenden Protokollen und den im Netzwerk verwendeten Applikationen und Programmen sind Zustände vorhanden, die dazu führen können ein Netzwerk zu stören. Im Folgenden sind dazu einige Möglichkeiten beschrieben[65][30][52].

2.2.1 Denial of Service (DoS)

Bei einer DoS-Attacke wird versucht, einen Dienst, einen Rechner oder auch eine ganzes Netzwerk zu blockieren. Dies kann unbewusst geschehen, in dem ein Kabel defekt ist oder versehentlich durch einen Konfigurationsfehler. Ganz gezielt ist dies jedoch auch mit diversen Möglichkeiten von Außen möglich.

Der Angreifer muss in der Regel nur versuchen, am entsprechenden Opfer einen so hohen Traffic zu erzeugen, dass es dem Opfer nicht mehr möglich ist auf andere Anfragen zu antworten. Wenn der Angreifer alleine ist, ist dies heutzutage nicht mehr ohne weiteres möglich, da die verfügbare Bandbreite mittlerweile in hohem Maß zur Verfügung steht. Der Angreifer muss also dafür sorgen, dass er über eine höhere Bandbreite als das Opfer verfügt. Dies gelingt ihm nur, indem er unter Zuhilfenahme weiterer Rechner (Bot-Netze) seine Kapazität erhöht. Diese Methode nennt sich Distributed DoS.

Ein DoS Angriff kann allerdings auch auf den TCP-Stack des Zielservers erfolgen, ein sogenannter SYN-Flood. Dabei versucht der Angreifer durch zufälliges Generieren einer idealer Weise nicht existenten IP-Adresse die Verbindungstabelle für offene Verbindungen zu füllen, indem er TCP/SYN Pakete für den Verbindungsaufbau generiert. Der angegriffene Rechner versucht zu antworten, kann diese Rechner aber aufgrund der nicht existenten IP-Adresse nicht erreichen. Die Verbindung wird aber in der Tabelle für die wartenden Verbindungen vorerst bleiben. Dies wiederholt der Angreifer solange bis die Tabelle voll ist und der Server diese löschen muss. Ist zwischendurch eine gültige Anfrage von einem existierenden Rechner gekommen wird diese auch entfernt, da der Server nicht zwischen diesen beiden unterscheiden kann. Für den normalen Besucher sieht es aus, als ob der Server nicht erreichbar ist[52, Kapitel 4.4.1][65, Kapitel 2.4.7].

2.2.2 Spoofing

Spoofing wird eine Methode genannt, die der Angreifer nutzt um Informationen zu fälschen. Dabei können die Informationen in unterschiedlichen Bereichen liegen. Nachfolgend sind die gängigen Methoden des Spoofings beschrieben. Daneben gibt es jedoch noch weitere Methoden auf denen Spoofing angewendet wird. Beim URL-Spoofing wird dem Besucher einer Website vorgetäuscht sich auf der Webseite seiner Wahl zu befinden, jedoch befindet er sich tatsächlich auf einer manipulierten Seite des Angreifers und gibt dort unter Umständen Bankinformationen preis, die der Angreifer abfängt. Beim Mail-Spoofing wird die Absenderadresse einer E-Mail gefälscht. Dies ist möglich, da das SMTP-Protokoll keine Überprüfung der Absenderadresse vorsieht. Der Empfänger erhält möglicherweise eine E-Mail mit Informationen, die nicht vom tatsächlichen Absender stammt. Ein verärgerter Kollege könnte eine E-Mail konzipieren und diese unter falschem Absender mit Betreff der Kündigung aus dem Unternehmen dem gemeinsamen Vorgesetzten senden[52, Kapitel 4.4.2].

IP-Spoofing

IP-Spoofing wird im Zusammenhang mit SYN-Floods benutzt um die eigene Identität zu verschleiern. Es kann aber auch dazu genutzt werden, einem Syslogd Server einen falschen Eintrag mitzuteilen,wenn dieser auf UDP-Basis arbeitet. TCP-Dienste sind vor gespooften Paketen sicher, da TCP verbindungsorientiert arbeitet und der Angreifer eine Sequenz- und Acknowledgenummer zusätzlich benötigen würde[52, Kapitel 4.4.2][30, Seite 45].

ARP-Spoofing

Da ein Angreifer in einem geswitchten Netzwerk einen Sniffer nicht sinnvoll einsetzen kann, bedient er sich an der Methode des ARP-Spoofings. Der Angreifer fälscht in diesem Fall den ARP-Reply einer ARP-Request-Anfrage eines Rechners. Möchte ein Rechner eine Verbindung mit einem anderen Rechner aufbauen, fragt dieser erstmal im Netz nach, welche MAC-Adresse der Ziel IP-Adresse entspricht. Der Switch wird diese Anfrage aufgrund der Anfrage an die Broadcast Adresse an alle angeschlossenen Ports weiterleiten. Die Antwort wird nun vom Angreifer mit seiner eigenen MAC-Adresse kommen. Der anfragende Rechner erhält die Antwort und sendet nun seine Datenpakete mit richtiger IP-Adresse, aber falscher MAC-Adresse. Da ein Switch jedoch nicht in der Lage ist, IP-Adressen auszuwerten, erhält der Angreifer die Daten. Allerdings kann der Angreifer diese nur annehmen, wenn er eine entsprechende Routingsoftware aktiviert hat. Dank der Routingsoftware kann er nun auch die Daten an den eigentlichen Zielrechner weiterleiten, er kennt ja die tatsächliche MAC-Adresse. Der Angreifer führt eine so genannte „Man in the Middle Attack“ durch und kann den Datenverkehr zwischen diesen zwei Rechnern abhören[52, Kapitel 4.4.2][30, Seite 48].

DNS-Spoofing

Ein DNS-Spoofing verläuft ähnlich wie das ARP-Spoofing. Hierbei wird dem anfragenden Rechner statt der gültigen IP-Adresse einer Bank, einem online Auktionshaus oder einer beliebigen Plattform mit Benutzerdaten, eine falsche IP-Adresse mitgeteilt. Der Angreifer muss allerdings zusätzlich noch einen Proxy-Server einrichten um die Anfragen an den echten Server weiterzuleiten. Der Angreifer befindet sich wiederum zwischen zwei Rechnern und kann den Datenverkehr zwischen Ihnen mitverfolgen[52, Kapitel 4.4.2][30, Seite 51].

2.2.3 Hijacking

Hijacking, im speziellen auch Session-Hijacking oder Telnet-Hijacking genannt, ist eine Methode, bei der der Angreifer versucht, eine bestehende Verbindung zu übernehmen. Ausgenutzt wird hierbei die Schwäche des TCP Protokolls. Bei einem Angriff werden eigene Pakete des Angreifers in die bestehende TCP-Verbindung eingeschleust. Die Sequenznummern werden durcheinandergebracht was zu einem ACK-Storm führt. Ein Denial of Service ist die Konsequenz. Dies muss jedoch in beiden Richtungen der Verbindung erfolgen. Vermieden werden kann solch ein Angriff durch ähnliche Gegenmaßnahmen wie beim Sniffing. Ein sternförmiges Netzwerk, welches mit Switchen realisiert wird, verhindert das Abhören einer Verbindung eines angegriffenen Rechners[52, Kapitel 4.4.3][30, Seite 50].

2.2.4 SQL-Injection

Eine SQL-Injection ist eine Möglichkeit, trotz einer sicher konfigurierten Firewall einen Zugriff auf schützenswerte Daten zu erhälten. Eine sinnvoll konfigurierte Firewall wird in vielen Fällen immer noch Anfragen für einen E-Mail-Server oder für eine Webseite durchlassen. Und hier befindet sich die Lücke. Eine SQL-Injection wird in der Regel über ein Web Formular durchgeführt. Der Angreifer trägt dazu beispielsweise in einem Formular zur Authentifizierung einen Benutzernahmen und im Passwortfeld eine weitere SQL-Anweisung wie etwa *';DROP TABLE KUNDE–* ein. So kann der Angreifer ganze Tabellen von fremden Datenbanken löschen. Vorausgesetzt ist jedoch, das der Datenbankbenutzer mit dem auf die Datenbank zugegriffen wird ausreichende Rechte besitzt und der Angreifer Kenntnis über die Struktur der Datenbank hat[1][52, Kapitel 4.4.7].

2.3 Schutzmöglichkeiten durch Firewall Architektur

Für die unterschiedlichsten Arten der Angriffe gibt es auch unterschiedliche Arten der Gegenmaßnahmen. Reicht es für den einen Angriff beispielsweise aus, bestimmte Ports zu blockieren, oder IP-Adressen nach Außen zu tarnen, ist es für andere Dienste erforderlich, dass der Datenstrom untersucht werden muss. Etwa um Viren zu erkennen oder einen Phishingversuch aus einer Webseite heraus zu erkennen.

2.3.1 Paketfilter

Ein Paketfilter ist eine Methode, die anhand eines Regelsatzes bestimmte Pakete einer Verbindung erlaubt und andere verwirft. Die Realisierung erfolgt durch iptables. Die Regeln werden anhand von Zieladresse, -port und bestimmter Flags der Verbindung erstellt. Eine Verschärfung des Paketfilters ist der „Stateful Paket Filter“. Bei dieser Methode wird eine weitere Regel hinzugefügt, die davon abhängig ist, welche Pakete vor dem aktuellen Paket gesendet wurden. Ab dem Linuxkernel 2.4.0 wird diese Methode unterstützt. Sie entscheidet beispielsweise, ob das Paket eine neue Verbindung öffnet, es zu einer bestehenden Verbindung gehört oder gar bereits in Beziehung zu einer anderen bestehenden Verbindung gehört. Die Abbildung 2.1 zeigt eine vereinfachte Darstellung des Paketfilters[52, Kapitel 2.1][30, Seite 65][65, Kapitel 2.1].

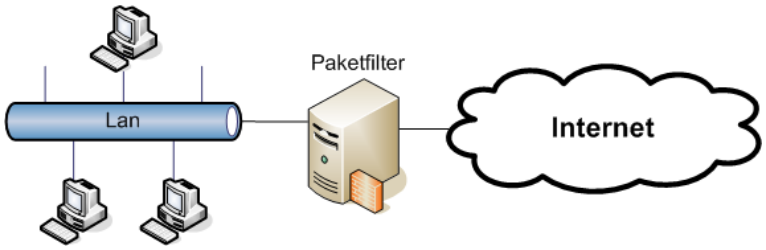


Abbildung 2.1: Schematische Darstellung eines Paketfilters[30, Seite 65]

Die Implementierung eines Paketfilters ist relativ einfach und kostengünstig durchzuführen. Auf den eingesetzten Clients sind keine Änderungen durchzuführen und auch die Anwendungen bemerken den zwischengeschalteten Paketfilter nicht. Ein weiterer Vorteil ist der hohe Datendurchsatz. Auch bei einem recht aufwändigen Regelsatz ist eine Überprüfung der Pakete so schnell, dass eine Verzögerung des Datenstroms am Client nicht auffällt.

Von Nachteil bei einem Paketfilter ist jedoch die Tatsache, dass dieser keiner Intelligenz unterliegt. Ein Regelwerk kann den Datenstrom nicht analysieren. Dazu bedarf es einer anderen Technik, der des Proxies.

2.3.2 Proxy

Ein Proxy gaukelt dem jeweiligen Rechner vor, er sei das eigentliche Ziel. Er nimmt alle Anfragen an und reicht diese an den entsprechenden Rechner weiter. Allerdings dann in eigenem

Namen. Die Antwort, die der Proxy daraufhin erhält, wird bearbeitet und danach an den anfragenden Rechner weitergereicht. Abbildung 2.2 zeigt einen einfachen Proxy.

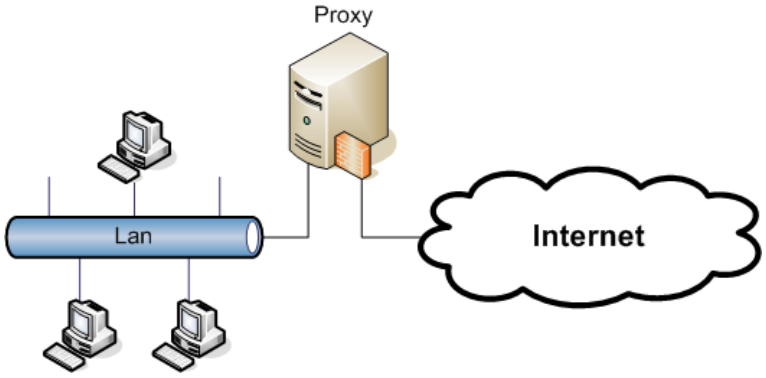


Abbildung 2.2: Schematische Darstellung eines Proxies[30, Seite 67]

Dies erlaubt eine sehr viel feinere Kontrolle des Datenstroms hat aber auch den Nachteil, dass dadurch eine sehr viel höhere Last durch die Interpretation des Datenstroms zwischen Gut und Böse entsteht. Auch ist ein Proxy nicht für jeden Dienst geeignet. Ein Proxy kann einfach mit den Protokollen HTTP, SMTP und DNS zusammenarbeiten. Jedoch bei einer FTP-Verbindung, welche das Protokoll einer Verbindung über einen Zwischenrechner nicht vorsieht, steht der Proxy vor einem Problem. Aber auch dafür gibt es eine Lösung. Entweder kennt der Client eine Methode wie er dem Proxy mitteilen kann, dass der Proxy selbst die FTP-Verbindung aufbaut oder er nutzt des SOCKS-Protokoll[30, Seite 68].

2.3.3 NAT - Network Address Translation

Die regelgesteuerte Manipulation der Absender- und/oder Empfängeradresse wird NAT bezeichnet. Dabei hat diese Technik im eigentlichen Sinn nichts mit einer Firewall zu tun. Der Umstand das NAT jedoch die IP-Adressen manipuliert und somit die Originaladressen verschleiert, wird gerne in einer Firewall mit eingesetzt. Die Umsetzung dieser Technik erfolgt in diesem Zusammenhang ebenfalls mit iptables womit schon der Paketfilter realisiert wurde[30, Seite 68].

NAT wird in zwei weitere Bereiche unterschieden. Zum einen in Destination-NAT, zum anderen in Source-NAT.

Source-NAT

Source-NAT wird die Veränderung der Quelladresse genannt. Dies geschieht im Allgemeinen, wenn ein Netzwerk ans Internet angeschlossenen wird. Das Netzwerk liegt dabei in einem nicht öffentlichen Netzbereich. Der Router sorgt nun dafür, dass jeder Rechner mit einer nicht offiziellen IP-Adresse nach außen für das Internet mit einer offiziellen IP-Adresse auftritt. Somit können etwa mehrere hundert Rechner unter einer einzigen Adresse im Internet agieren. Der Router muss dafür nur eine interne Liste führen, anhand dieser er die Verbindungen den internen Rechner zuordnen kann. Da der Router die Anfragen zum Internet selbst stellt, kann er auch den Absenderport manipulieren. Somit erhält er einen eindeutigen Schlüssel und kann diesen in seiner Tabelle eintragen. Erhält der Router eine Antwort auf diesem Port, schlägt er in seiner Tabelle nach und weiß an welchen internen Rechner er die Antwort schicken muss. Diese spezielle Technik wird auch Masquerading genannt[30, Seite 69].

Destination-NAT

Destination-NAT hingegen ist die umgekehrte Nutzung dieser Technik. Dabei wird ein interner Server, etwa ein firmeneigener Webserver der eine private IP-Adresse hat, für das Internet zugänglich gemacht. Der Router, der eine offizielle IP-Adresse hat und diese dem Domainnamen *www.domainname.de* zugeordnet ist, leitet nun alle Anfragen an die Adresse des eingetragen internen Servers weiter. Es wird somit eine Umleitung von einem Rechner auf einen anderen Rechner realisiert. Ein Spezialfall für Destination-NAT ist die Redirection. Die dabei bedeutendste Anwendung der Redirection ist die Einrichtung eines transparenten Proxies. Der Vorteil eines transparenten Proxies liegt zum einen im geringeren Administrationsaufwand, denn die Clients müssen nicht mehr speziell eingerichtet werden. Zum anderen wird ein gezieltes Aushebeln durch Umgehung des Proxies vom Client aus vermieden und ein weiteres Stück Sicherheit ist erreicht[30, Seite 70].

2.4 Einsatzszenarien und Konzepte

Eine Firewall besteht heutzutage nicht mehr aus einem reinen Proxy oder nur aus einem Paketfilter. Vielmehr wird auf die gezielte Kombination und somit der Ausnutzung der Vorteile der einzelnen Techniken gesetzt.

Eine Möglichkeit nennt sich Screened Host, wie in Abbildung 2.3 dargestellt. Diese Kombination stellt zum einen sicher, dass durch den Einsatz der Paketfilter nur als sicher gekennzeichnete Pakete in Netzwerk kommen. Zum anderen werden Verbindungen ins Internet nur durch den Proxy aufgebaut, bzw. gelangen von außen erst auf diesen. Ebenso ist durch den Paketfilter gewährleistet, dass nur erlaubte Protokolle aus dem LAN direkt ins Internet gehen.[30, Seite 71]

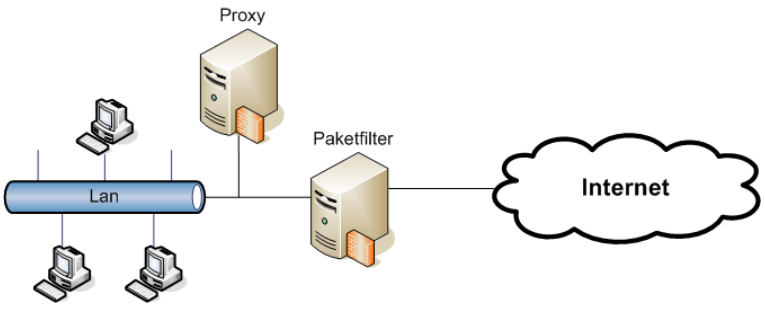


Abbildung 2.3: Schematische Darstellung eines Screened Host[30, Seite 71]

Ein weiteres Konzept wird jedoch notwendig, sobald eigene Serverdienste aus dem Intranet angeboten werden. Ein kompromittierter Webserver würde das Konzept des Screended Host umgehen, da er, sobald er auf dem Webserver Zugriff hat, auch Zugang zum LAN bekommt. Die dazu bevorzugte Lösung nennt sich Screened Subnet, wie sie in Abbildung 2.4 dargestellt ist. Dazu wird der Proxy zwischen zwei Paketfilter gesetzt. Es entsteht ein weiteres Netzwerk, die DMZ auch demilitarisierte Zone genannt. Dies ist dann der ideale Ort für Web-, FTP- oder E-Mail-Server, da dieser Bereich durch den zusätzlichen Paketfilter vom internen LAN getrennt ist. Durch zusätzliches Einfügen weiterer Paketfilter können somit zusätzliche Bereiche definiert werden, die voneinander getrennt sind und somit zu einem höheren Schutz beitragen[30, Seite 72].

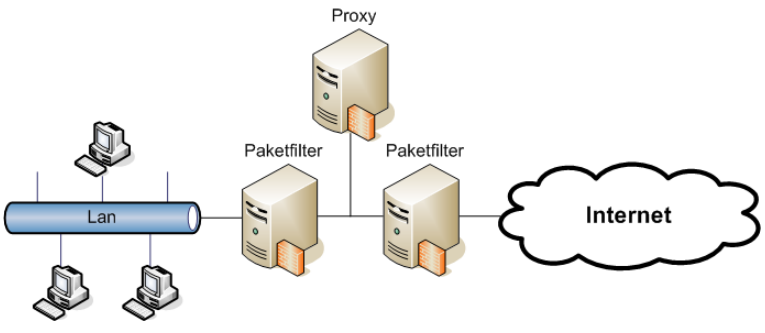


Abbildung 2.4: Schematische Darstellung eines Screened Subnet[30, Seite 72]

Die im IPCop eingesetzte Variante ist eine leicht modifizierte Variante des Screened Subnet

in der äußerer und innerer Paketfilter zusammengelegt sind. Dazu bekommt der eingesetzte Firewall Rechner drei Netzwerkkarten, von denen eine mit dem Internet, eine mit dem LAN und die dritte mit der DMZ verbunden ist. Bei dieser Variante ist jedoch eine sorgfältige Planung und Aufstellung der Paketfilterregeln erforderlich. Auch wenn diese Variante an einen Screened Host erinnert, so befindet sich zwischen LAN und Internet sowie LAN und Proxy ein reiner Paketfilter.

3 IPCop

IPCop entstand im Oktober 2001 als Fork aus dem kommerziellen Projekt SmoothWall und basiert auf Version v0.9.9. Bis zur Version 1.3.x basierte das Projekt aus diesem Grund auch auf der Linux-Disitribution RedHat. Mit der Version 1.4 wurde die Linux Basis auf LFS (Linux from Scratch) umgestellt, also der Generierung eines Linux-Systems aus dem Linux-Quellcode.

Auf die Fragehin, was IPCop eigentlich ist, lässt sich im Administrationshandbuch folgendes lesen:

> 1. IPCop ist eine Firewall; zu aller erst, zuletzt und überhaupt.
> 2. IPCop ist eine spezialisierte Linux Distribution; komplett, konfiguriert, und fertig um Ihr Netzwerk zu schützen. Ferner, es fällt unter die GNU General Public License [http://www.gnu.org/licenses/gpl.html], d.h. der komplette Quellcode kann heruntergeladen und überprüft werden, oder einfach von Ihnen für Ihre persönlichen Vorlieben oder aus eigenen Sicherheitsgründen modifiziert und/oder rekompiliert werden.
> 3. IPCop ist eine Community; wo Mitglieder einander helfen und alle sich beteiligen das Projekt und sich gegenseitig zu verbessern. Diese Unterstützung beginnt beim simplen # „Networking 101“#-Typ durch Instruktionen und Anweisungen bis hin zur Hilfestellung für Mitglieder beim Anpassen ihrer IPCop um spezielle Bedürfnisse wie z.B. Net-Phones (VoIP) oder Multiple-Büro-Integrität zu bewältigen.[37]

Die Abspaltung als eigenes Projekt aus dem bestehenden Projekt Smoothwall hatte mehrere Gründe. Als die Software 2001 als reine Firewall entwickelt wurde bestand der Wunsch der Entwickler eine Firewall zu entwickeln, die im Gegensatz zu den bis dahin verfügbaren Firewalls zum einen unter der GNU General Public License fällt, sowie der entwickelten Software eine Community zur Verfügung zu stellen. Die SmoothWall wurde kommerziell und stand in der frei verfügbaren Version nur in einem eingeschränkten Funktionsumfang zur Verfügung.

Die Entwickler hatten die Befürchtung, dass durch die Kommerzialisierung des Projekts die Entwicklung beeinträchtigt würde.

Mittlerweile hat sich aus dem IPCop-Projet ein weiterer Fork gebildet, die Endian-Firewall. Diese vereint die Basisfunktionen des IPCops sowie einiger ausgewählter AddOns in einer Distribution. Hinter dem Projekt steht die Firma Endian s.r.l mit Sitz in Italien. Die Software unterliegt ebenfalls der GPL und ist ebenso frei verfügbar, wird jedoch kommerziell mit gebündelter eigener Hardware als Komplettlösung vertrieben. Verkauft wird demnach die Hardware und der Support[53].

3.1 Netzwerk

IPCop unterteilt grundsätzlich in verschiedene Netzwerkschnittstellen[2, Seite 48], siehe Abbildung 3.1. Auffällig dabei ist die Ampelkonstellation, die in gewisser Weise die Gefahr transparent darstellt. Grün ist das sichere Lokale Netzwerk, rot hingegen ist das gefährliche Internet von der die Bedrohung ausgeht und vor dem das grüne Netz geschützt werden soll. Orange bedeutet dagegen einen gewissen Schutz mit eventuellen Risiken und Gefahren und steht somit für die DMZ. Die Farbe blau ist nicht assoziiert mit einer Bedeutung für Gefahr oder Sicherheit. Blau steht indes für eine Funkverbindung.

Dabei gilt nach der Installation das Regelwerk wie es aus der Tabelle 3.2 zu entnehmen ist.

In der Grundkonfiguration steht dem Benutzer bereits ein sicheres System zur Verfügung. Jeder Verkehr von außerhalb nach innen wird abgeblockt, umgekehrt jedoch ist alles offen. Somit kann der Benutzer bereits auf Internetdienste zugreifen ohne befürchten zu müssen, dass sein Netzwerk Angriffen ausgesetzt wird. Sobald es erforderlich ist, dass ein Webservice angeboten wird, oder von außerhalb ein VPN-Zugang eingerichtet oder via Remote Desktop Protokoll (RDP) auf interne Rechner zugegriffen werden muss, kann und muss dieses Regelwerk auch durch Konfigurationseinstellungen gehärtet beziehungsweise aufgelockert werden. Es lässt sich individuell auf die eigenen Bedürfnisse anpassen. Ebenso kann auch durch ein AddOn (BlockOut Traffic), der Verkehr von innen nach außen, der wie in der Tabelle 3.2 dargestellt offen ist, geschlossen und reglementiert werden.

Tabelle 3.1: Schnittstellen im IPCop[5, Kapitel 1.2.1]

Schnittstelle	Funktion	Beschreibung
Rot:	Externes Netz	Über diese Schnittstelle wird die Internetverbindung hergestellt. Der IPCop schützt die anderen Schnittstellen vor dieser nicht vertrauenswürdigen Schnittstelle.
Orange:	Demilitarisierte Zone - DMZ	An dieser Schnittstelle sind alle diejenigen Server angebunden, die Dienste im Internet bereitstellen (Webserver, E-Mail-Server, ftp-Server, ...) Datenverkehr ins Internet ist möglich, jedoch nicht ins grüne Netzwerk. Dies wird nur über die DMZ-Pinholes möglich.
Grün:	Internes Netz	Dieser Bereich ist durch IPCop besonders geschützt. Innerhalb dieses Netzwerks befinden sich alle Clients. Er ist vor Zugriffen aus den anderen Bereichen geschützt.
Blau:	Wireless Lan - WLAN	Über diese Schnittstelle werden WLAN-Geräte betrieben. Er kann mit dem grünen Netzwerkverglichen werden, mit dem unterschied das von hier aus kein direkter Zugriff auf alle anderen Schnittstellen möglich ist. Dieser muss separat über Regeln definiert werden.

Tabelle 3.2: Regelwerk im IPCop[37, Kapitel2.6.1]

Quelle		Ziel	Status	Zugriffsmethode
Rot	>	Firewall	Geschlossen	externer Zugang
Rot	>	Orange	Geschlossen	Port-Weiterleitung
Rot	>	Blau	Geschlossen	Port-Weiterleitung oder VPN
Rot	>	Grün	Geschlossen	Port-Weiterleitung oder VPN
Orange	>	Firewall	Geschlossen	Kein DNS oder DHCP
Orange	>	Rot	Offen	
Orange	>	Blau	Geschlossen	DMZ-Schlupflöscher
Orange	>	Grün	Geschlossen	DMZ-Schlupflöscher
Blau	>	Firewall	Geschlossen	Zugriff auf Blau
Blau	>	Rot	Geschlossen	Zugriff auf Blau
Blau	>	Orange	Geschlossen	Zugriff auf Blau
Blau	>	Grün	Geschlossen	DMZ-Schlupflöscher oder VPN
Grün	>	Firwall	Offen	
Grün	>	Rot	Offen	
Grün	>	Orange	Offen	
Grün	>	Blau	Offen	

3.2 Netzwerkkonfiguration

Je nach vorhandener IT-Infrastruktur ergeben sich unterschiedliche Netzwerkarchitekturen. In den nachfolgenden Abbildungen werden exemplarisch drei Möglichkeiten von Netzwerken und ihrer Anbindung ans Internet dargestellt.

Abbildung 3.1 zeigt ein Netzwerk mit zwei Schnittstellen. Dies ist die klassische Anbindung wie sie in vielen privaten Haushalten oder kleinen Büros erfolgt. Der IPCop enthält zwei Netzwerkkarten. Die Einwahl ins Internet erfolgt über ein DSL-Modem, oder über eine Analog/ISDN Wählverbindung. Der IPCop erhält bei der Einwahl vom Provider eine dynamische IP-Adresse. Alle weiteren Einstellungen (DNS-Server, Gateway) erhält er ebenfalls vom Provider. Die Konfiguration des Netzwerks erfolgt manuell. Das Gateway für die Clients ist der IPCop. Dieser ist ebenfalls DNS-Server, da er die DNS-Anfragen an den vom Provider zugewiesenen DNS-Server weiterleitet[2, Seite 69].

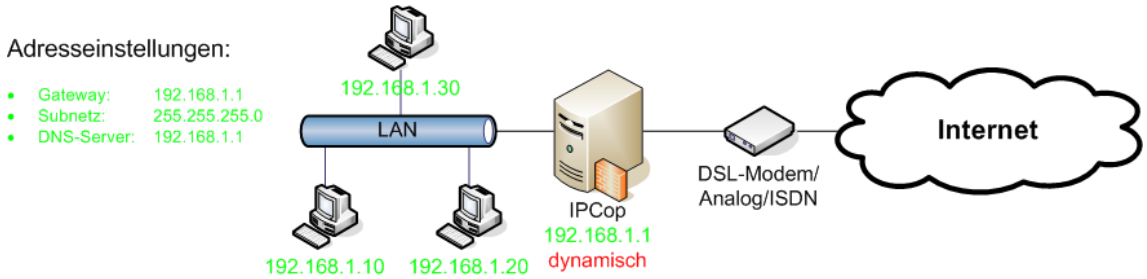


Abbildung 3.1: Netzwerk mit Anbindung über ein Modem (Dynamische IP-Adresse)[2, Seite 69]

Die zweite Abbildung, zeigt die gleiche Konfiguration wie bereits oben beschrieben. Hier erfolgt die Einwahl jedoch nicht vom IPCop aus, sondern über einen separaten Router. Oft werden DSL-Modems mit bereits integriertem Router vertrieben, welche die Einwahl ins Internet selbst übernehmen. In diesem Fall wird der IPCop mit einer statischen IP-Adresse auf der roten Schnittstelle konfiguriert. Es muss nun jedoch auch das Gateway und der DNS-Server im IPCop konfiguriert werden. Dies ist die Adresse des Routers. Alternativ, kann als DNS-Server auch ein bekannter externer DNS-Server des Providers angegeben werden.

Erfolgt die Einrichtung des Netzwerks in einem größere Unternehmen kann es durchaus notwendig sein E-Mail-Server und/oder Webserver mit zu integrieren. In diesem Fall wird die Einrichtung einer DMZ notwendig. Der IPCop enthält nun drei Netzwerkkarten. Die Netze sind somit alle physikalisch voneinander getrennt[2, Seite 73].

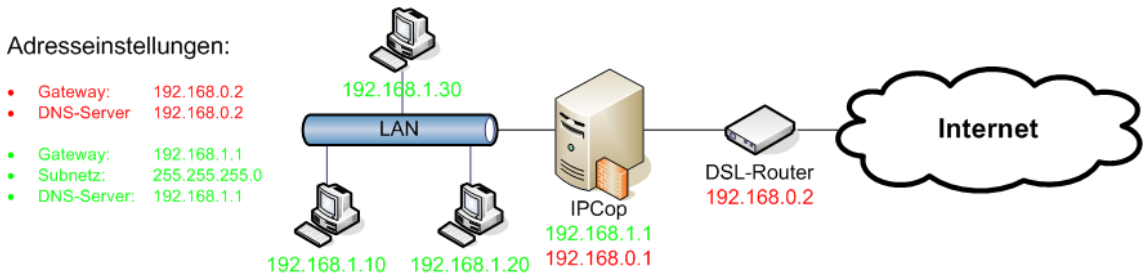


Abbildung 3.2: Netzwerk mit Anbindung über einen Router (Statische IP-Adresse)

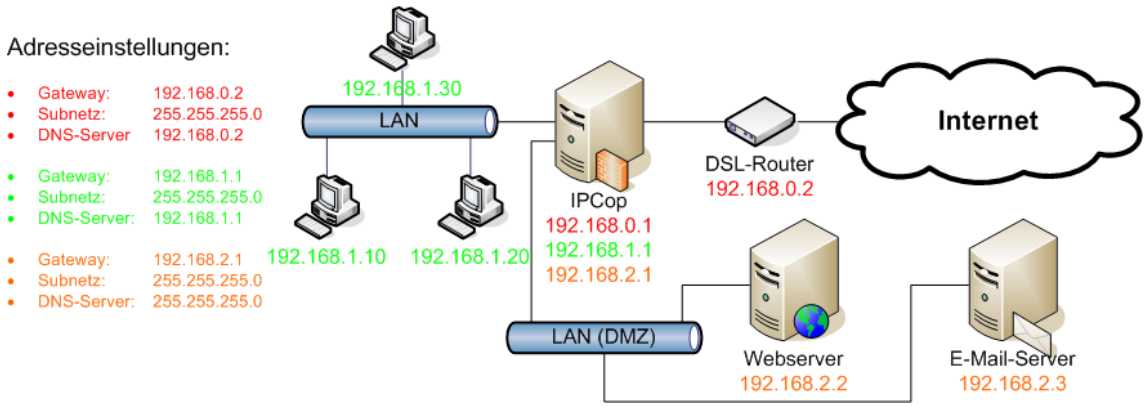


Abbildung 3.3: Netzwerk mit einer DMZ[2, Seite 73]

3.3 Funktionsumfang

Das Installationspaket hat bereits einen gut ausgestatteten Funktionsumfang. Neben einer Weboberfläche zur komfortablen Konfiguration und Überwachung der Firewall existiert eine umfangreiche Liste an Hardwarekomponenten die unterstützt werden[27]. Dazu gehören unter anderem zahlreiche Netzwerkkarten, diverse analoge Modems und ADSL-Modems.

Weiterhin enthält die Firewall einen einfachen WebProxy, einen DHCP-Dienst, einen DNS-Server, einen Zeitserver, unterstützt Dynamisches-DNS, VPN, Port-Forwarding und erweiterte Netzwerkdienste wie Intrusion Detection und Traffic Shaping.

3.4 Installation

Die Installation gestaltet sich dank einer ausgeklügelten Installationsroutine und einem ausführlich beschriebenen und mit Abbildungen versehenen Handbuch[5] als überaus einfach

und schnell. Sofern die Planung abgeschlossen ist und die Konfiguration feststeht dauert die Installation rund 15 Minuten. Ist bereits eine Installation vorhanden, kann durch Einspielen noch während des Installationsvorgangs einer vorher erstellten Backupdatei die letzte Konfiguration direkt mit eingespielt werden.

Die Installation kann auf drei unterschiedliche Arten erfolgen[5, Kapitel 1.5].

- Bootfähige CD
- Bootfähige Diskette + CD
- Bootfähige Diskette + FTP/WebServer

Eine genaue Beschreibung, insbesondere der Feinheiten bei abweichender Standardinstallation, kann der Installationsanleitung auf der Projektseite entnommen werden.

3.4.1 Hardwarevoraussetzungen

Die Hardwarevoraussetzungen sind in der Schnellstartanleitung [6] angegeben. So wird ein Prozessor in x86 Architektur angegeben. Mindestens wird jedoch ein 386 Prozessor mit einer Ausstattung von 32 MB Arbeitsspeicher und einer 300 MB Festplatte vorausgesetzt. Dies setzt allerdings voraus, dass auf den Einsatz performancelastiger Dienste wie WebProxy oder IDS verzichtet wird. Werden trotzdem diese Dienste in Anspruch genommen, werden ein schnellerer Prozessor, mehr Arbeitsspeicher und eine größere Festplatte nötig.

Weiterhin ist es sinnvoll, ein Diskettenlaufwerk und/oder ein CDROM Laufwerk einzusetzen. Beides erleichtert die Installation, ist jedoch nicht erforderlich, da diese auch übers Netzwerk erfolgen kann. Auch kann das Diskettenlaufwerk als Backupmedium verwendet werden, wobei seit der Version 1.4.11 auch auf einen USB-Datenträger gesichert werden kann.

In jedem Fall wird jedoch mindestens eine Netzwerkkarte benötigt, sofern die Internetverbindung über ein Modem oder ISDN-Karte aufgebaut wird. Ansonsten werden je nach Netzwerktopologie mindestens zwei oder drei Netzwerkkarten benötigt.

Zusätzlich ist es möglich IPCop auf einer CompactFlash Speicherkarte zu installieren. Dazu ist jedoch ein gesondertes IsoImage MKflash [66] erforderlich. CompactFlash Speicherkarten haben die Eigenart nur eine gewisse Anzahl an Schreibvorgängen zu überstehen und nur bei rund 100.000 Zugriffen [54, Seite 9] pro Speicherzelle liegen. Die Schreibzugriffe sollten soweit wie möglich minimiert werden. Daher wurde die Original Distribution für CompactFlashkarten angepasst. Ebenso sorgt ein Algorithmus in der CompactFlash-Karte dafür, dass

nicht immer die gleichen Speicherzellen beschrieben werden. Angepasste Versionen sind auf der deutschen Community Plattform im Downloadbereich verfügbar.

Nach der Installation können CD-ROM, Tastatur und Monitor vom Rechner entfernt werden. Die Wartung und Konfiguration erfolgt nun ausschließlich über das Netzwerk, entweder über das Webfrontend oder über einen Shellzugang.

3.4.2 Installationsvorgang

Am einfachsten gestaltet sich die Installation mit einer bootfähigen Installations-CD. Nachdem diese ins CD-Laufwerk eingelegt und der Rechner gestartet wurde erscheint ein Informationsbildschirm mit einer Warnung[5, Kapitel 2.1], dass alle Daten auf der eingebauten Festplatte gelöscht werden. Nach Bestätigung mit *Enter* startet der Bootvorgang des Linux-Systems und das Setup wird gestartet. Es erscheint nun als erstes eine Auswahlmaske zur Einstellung der Sprache. Nach gewünschter Wahl folgt eine Begrüßung des Benutzers zum Installationsprogramm. Durch Bestätigung wird der Benutzer gefragt, von welchem Quellmedium er das System installieren möchte. Nach Auswahl der Option *CDROM* erfolgen die Partitionierung der Festplatte und die Erstellung des Dateisystems. Dieser Vorgang dauert je nach ausgestatteter Hardware mehrere Sekunden bis wenige Minuten.

Sobald dieser Vorgang abgeschlossen ist, besteht die Möglichkeit ein vorhandenes Backup nach Bedarf einzuspielen. Nach der Wiederherstellung ist der Installationsvorgang beendet.

Soll keine Systemwiederherstellung durchgeführt werden, folgt die Konfiguration der Netzwerkkarte für das lokale grüne Netzwerk. In der Regel werden alle gängigen Karten automatisch erkannt. Schlägt die automatische Erkennung fehl, besteht zusätzlich die Möglichkeit der manuellen Einrichtung durch Angabe des Modulnamens und der benötigten Parameter für den ausgewählten Treiber. Wird die Karte erfolgreich erkannt, schließt die Installation nach Eingabe der IP-Adresse *192.168.150.1* und Subnetzmake *255.255.255.0* für das lokale Netzwerk. Der Benutzer erhält einen letzten Hinweis darüber, dass die Installation erfolgreich verlaufen ist, er alle Medien aus bootfähigen Laufwerken zu entfernen hat und anschließend das Konfigurationsprogramm gestartet wird.

Abbildung 3.4 zeigt exemplarisch einige Screenshots der Installation und Konfigurationsdialoge.

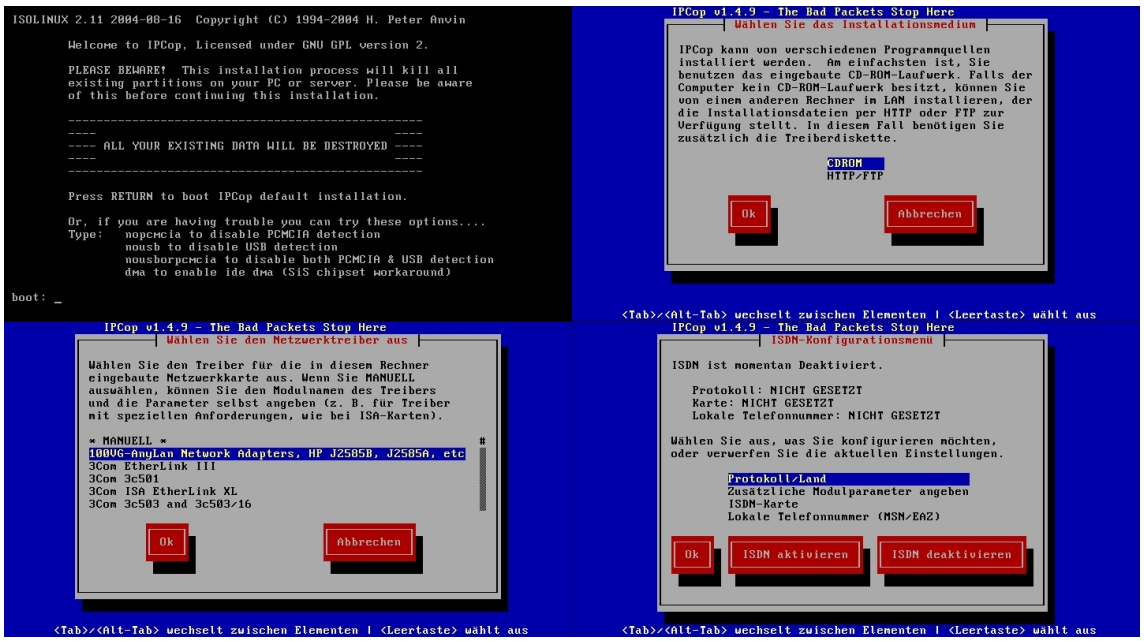

ISOLINUX 2.11 2004-08-16 Copyright (C) 1994-2004 H. Peter Anvin
Welcome to IPCop, Licensed under GNU GPL version 2.
PLEASE BEWARE! This installation process will kill all existing partitions on your PC or server. Please be aware of this before continuing this installation.
ALL YOUR EXISTING DATA WILL BE DESTROYED
Press RETURN to boot IPCop default installation.
Or, if you are having trouble you can try these options....
Type: nopcmcia to disable PCMCIA detection
nousb to disable USB detection
nousborpcmcia to disable both PCMCIA & USB detection
dma to enable ide dma (SiS chipset workaround)
boot:
IPCop v1.4.9 - The Bad Packets Stop Here
Wählen Sie das Installationsmedium
IPCop kann von verschiedenen Programmquellen installiert werden. Am einfachsten ist, Sie benutzen das eingebaute CD-ROM-Laufwerk. Falls der Computer kein CD-ROM-Laufwerk besitzt, können Sie von einem anderen Rechner im LAN installieren, der die Installationsdateien per HTTP oder FTP zur Verfügung stellt. In diesem Fall benötigen Sie zusätzlich die Treiberdiskette.
CDROM
HTTP/FTP
Ok
Abbrechen
<Tab>/<Alt-Tab> wechselt zwischen Elementen | <Leertaste> wählt aus
IPCop v1.4.9 - The Bad Packets Stop Here
Wählen Sie den Netzwerktreiber aus
Wählen Sie den Treiber für die in diesem Rechner eingebaute Netzwerkkarte aus. Wenn Sie MANUELL auswählen, können Sie den Modulnamen des Treibers und die Parameter selbst angeben (z. B. für Treiber mit speziellen Anforderungen, wie bei ISA-Karten).
* MANUELL *
100VG-AnyLan Network Adapters, HP J2585B, J2585A, etc
3Com EtherLink III
3Com 3c501
3Com ISA EtherLink XL
3Com 3c503 and 3c503/16
Ok
Abbrechen
<Tab>/<Alt-Tab> wechselt zwischen Elementen | <Leertaste> wählt aus
IPCop v1.4.9 - The Bad Packets Stop Here
ISDN-Konfigurationsmenü
ISDN ist momentan Deaktiviert.
Protokoll: NICHT GESETZT
Karte: NICHT GESETZT
Lokale Telefonnummer: NICHT GESETZT
Wählen Sie aus, was Sie konfigurieren möchten, oder verwerfen Sie die aktuellen Einstellungen.
Protokoll/Land
Zusätzliche Modulparameter angeben
ISDN-Karte
Lokale Telefonnummer (MSN/EAZ)
Ok
ISDN aktivieren
ISDN deaktivieren
<Tab>/<Alt-Tab> wechselt zwischen Elementen | <Leertaste> wählt aus

Abbildung 3.4: Screenshots der Installations- und Konfigurationsdialoge

Erstkonfiguration

Nach erfolgreicher Installation und automatischem Start erscheint nun erstmalig das Konfigurationsprogramm im Assistentenmodus[5, Kapitel 3]. Dieses ist später jederzeit wieder durch Eingabe des Befehls *setup* auf der Kommandozeilenoberfläche aufrufbar. Zuerst wird die Eingabe des verwendeten TastatURLayouts gefordert. Danach erfolgt die Auswahl der Zeitzone, in der sich der IPCop Rechner befindet.

Als nächstes erfolgt die Vergabe eines Namens für den IPCop-Rechner, sowie die Festlegung in welcher Domäne sich der IPCop Rechner befindet. Der vorgeschlagene Namen *IPCop* kann übernommen werden, ebenfalls der Domainname *localdomain* sofern keine Domain vorhanden ist.

Schließlich fährt das Konfigurationsprogramm mit der Netzwerkkonfiguration fort. Es erscheint die Auswahl zur ISDN-Konfiguration. Sofern ISDN nicht benötigt ist, wird dieser Schritt übersprungen. Andernfalls erfolgt die Auswahl des Protokolls, die Einrichtung des Treibers, die Auswahl der verwendeten ISDN-Karte und die Vergabe der Telefonnummer.

Wird ISDN nicht verwendet, ist die Konfiguration mindestens einer weiteren Netzwerkkarte erforderlich. Je nach gewünschtem Typ des Netzwerks können bis zu vier Netzwerkschnittstellen konfiguriert werden. Es folgt nun die Angabe der IP-Adressinformationen für die externe

rote Schittstelle. Dies kann entweder statisch oder dynamisch über DHCP vergeben werden. Auch ist eine Einwahl über PPPOE oder PPTP möglich.

Wird die Firewall an einem Gateway betrieben, also die rot Schnittstelle hat eine statische IP-Adresse bekommen, erfolgt nun noch die Angabe der primären und/oder sekundären DNS-Adresse(n), sowie die Angabe des Gateways.

Falls der IPCop im lokalen Netzwerk selbst einen DHCP-Dienst für die lokalen Rechner anbieten soll, müssen in der nächsten Maske die Option 'aktiviert' gewählt und die entsprechenden Parameter konfiguriert werden. Falls nicht wird die Maske nur mit OK bestätigt.

Die letzten Schritte innerhalb der Erstkonfiguration sind die Festlegung der Passwörter für den Shell-Zugang *root* sowie für den Benutzer des Webinterfaces *admin*. Hier sollten in jedem Fall zwei komplexe, unterschiedliche Passwörter definiert werden. Die Erstkonfiguration ist damit abgeschlossen.

3.4.3 IPCop in virtuellen Maschinen

Durch den Einsatz einer Virtualisierungssoftware wie etwa VMware, Xen und anderen ist es möglich, IPCop auf einem Host-System laufen zu lassen ohne für diesen eine separate Hardware bereitzustellen. Im Projet *cf Server* wurde diese Methode zuerst mit IPCop umgesetzt. In der neuen Version des *cf Servers* wird nun aufgrund eines Wechsel des Kernels die Endian Firewall eingesetzt[38, Seite 133]. Obwohl der Einsatz in dieser Art möglich ist, bricht dieser Aufbau die grundsätzlichen Regeln die in einem Firwallkonzept zur Sicherheit beitragen sollen.

Eine Firewall ist sicher, vorausgesetzt die Firewallsoftware selbst unterliegt keinem Fehler. Dies liegt daran, dass nur Dienste angreifbar sind, die angeboten werden. Wird ein Angriff auf einen Webserver gefahren, schlägt dieser bereits fehl, wenn kein Webserver antworten kann, weil dieser nicht aktiviert und so nicht erreichbar ist. Eine Gefahr im Betrieb einer Firewall in einer virtuellen Umgebung liegt nun zum einen darin, dass alle Datenpakete die zur Firewall müssen, erst einmal das Hostsystem durchlaufen. Dies wird zwar durch die Verwendung eigener IP-Stacks, die keine direkte Verbindung zwischen Host- und Gastsystem erlauben, unterbunden, aber ein Fehler innerhalb des IP-Stacks ist wie in jeder Software möglich. Somit wäre etwa ein Angriff auf ein virtuelles System denkbar. Eine weitaus höhere Gefahr geht

jedoch von den Diensten auf dem Hostsystem aus. Ist dort ein Dienst kompromittiert worden, hat der Angreifer direkten Zugriff auf das gesamte System einschließlich der Firewall[63].

Der grundsätzliche Einsatz einer Firewall, unabhängig ob IPCop oder ein anderes Produkt in einem virtuellen System, ist definitiv nicht ratsam und sollte in keiner produktiven Umgebung Verwendung finden. In einer Test- oder Entwicklungsumgebung spricht allerdings nichts gegen einen solchen Einsatz, da hier die Vorteile der gemeinschaftlichen Nutzung eines einzigen Rechners zum Tragen kommen.

4 Konfiguration und Einrichtung der Basismodule

Nach der Installation folgt die Konfiguration des IPCops, obwohl dieser prinzipiell bereits einsatzbereit ist und das dahinter liegende Netzwerk schützt. Der nachfolgende Teil beschäftigt sich zunächst mit den Basismodulen, die sich im Lieferumfang befinden. Im darauf folgenden Kapitel folgt die Installation und Einrichtung ausgewählter Zusatzmodule die den Funktionsumfang des IPCops wesentlich erweitern können und in einem hohen Maß zur zusätzlichen Sicherheit beitragen.

Nach erfolgreicher Installation gelangt der Benutzer auf die Weboberfläche des IPCops über die bei der Installation festgelegten Adresse für das grüne Netzwerk. Wichtig ist die Angabe des Ports, da die SSL-Verbindung nicht über den Standardport 443 sondern über den Port 445 hergestellt wird. Der Adressaufruf könnte so aussehen: `https://192.168.150.1:445`. Das WebGUI der Firewall zeigt einen Startbildschirm 4.1 mit einigen allgemeinen Informationen (Benutztes Profil, IP-Adresse, Hostname des IPCops, Verbindungsstatus, Uptimes sowie die Systemauslastung).

Dieser Bildschirm ist jederzeit aus dem grünen Netzwerk erreichbar. Durch Auswahl eines Menüpunkts oder eines Klicks auf einen der beiden Button für *Verbinden* oder *Trennen* erscheint eine Loginmaske. Der Benutzer in diesem Fall ist *admin* und das Passwort ist jenes, welches bei der Installation vergeben wurde. Der Button *Aktualisieren* erfordert kein Login.

4.1 Allgemeine Einstellungen

Über das Menü System gelangt der Benutzer zu den Punkten *Startseite*, *Updates*, *Passwörter*, *ssh-Zugriff*, *Einstellungen der Benutzeroberfläche*, *Datensicherung*, *Herunterfahren* und dem Punkt *Dank an...*.

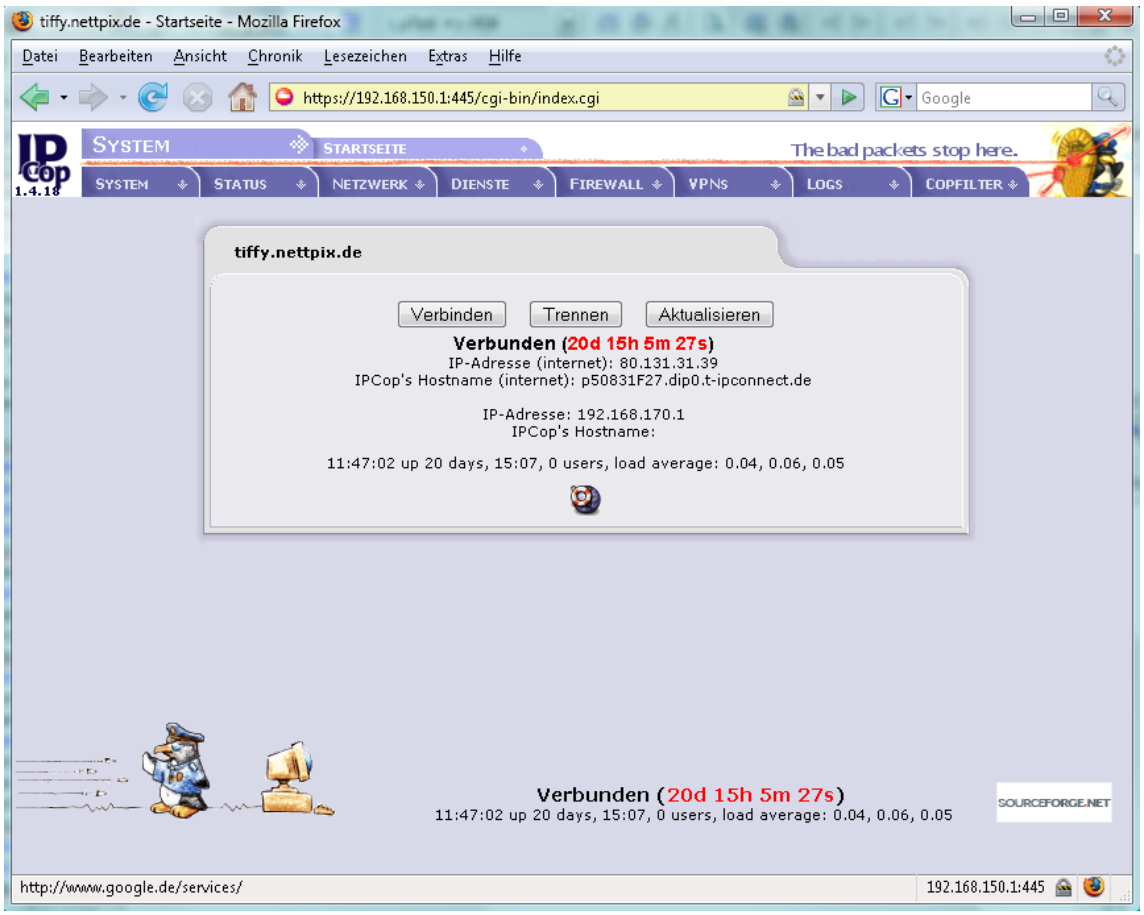


Abbildung 4.1: Screenshot des IPCop-Startbildschirm

4.1.1 Updates

In der aktuellen Version 1.4.18 wurde der Punkt Updates erneuert. Dem IPCop ist es nun möglich, direkt aus der Weboberfläche heraus neu angekündigte Updates direkt herunterzuladen und zu installieren. In den früheren Versionen war nur die automatische Ankündigung implementiert. Das Update musste manuell heruntergeladen und vom WebGUI aus hochgeladen werden. Ebenfalls neu ist die absteigende Sortierreihenfolge der bereits installierten Updates[37, Kapitel 2.1.1].

4.1.2 Passwörter

Auf diesem Bildschirm können die Passwörter für den administrativen Webzugang *admin* sowie dem eingeschränktem Webnutzer *dial* geändert werden. Der Benutzer *dial* hat nur das

Recht eine Verbindung zu beenden und erneut aufzubauen. Er steht zudem nur zur Verfügung, wenn der IPCop zur Einwahl konfiguriert wurde. Dies bietet sich an, wenn der Administrator den Benutzern erlauben möchte, die Verbindung zu steuern ohne ihnen administrative Rechte zu geben. Der Bentzer *root* für den Shellzugriff kann nur direkt über eine Konsole im Setupprogramm geändert werden[37, Kapitel 2.1.2].

4.1.3 SSH-Zugriff

Hinter diesem Menüpunkt verbirgt sich die Einstellung, ob eine Verbindung über eine Console via Putty oder Ähnliches erlaubt ist. Ebenso werden hier die Einstellungen zur Authentifizierung über SSH konfiguriert. Wichtig in diesem Zusammenhang ist, dass der SSH-Dienst auf Port 222 und nicht auf dem Standard Port 22 läuft. Abbildung 4.2 zeigt eine solche Verbindung[37, Kapitel 2.1.3].

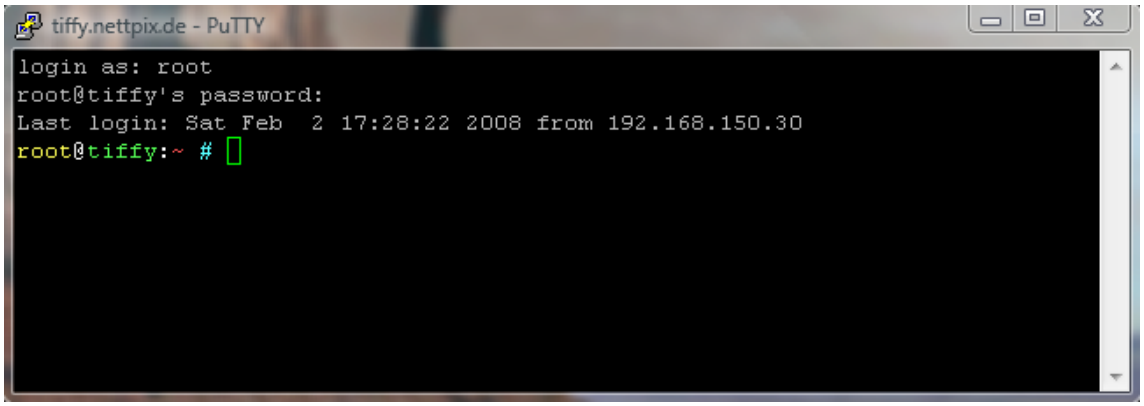


Abbildung 4.2: Screenshot der SSH-Verbindung mit Putty

4.1.4 Einstellungen der Benutzeroberfläche

Unter diesem Punkt wird die Benutzeroberfläche konfiguriert. Da gewisse Browser unter Umständen kein JavaScript unterstützen oder es im Browser deaktiviert ist, kann diese Funktion deaktiviert werden. Auch ist auf diesem Bildschirm die bevorzugte Sprache anpassbar. Weiterhin wird hier konfiguriert ob der Hostname auf der Startseite angezeigt wird und ob der IPCop bei einer Änderung des Verbindungszustands einen Signalton von sich gibt[37, Kapitel 2.1.4].

4.1.5 Datensicherung

Im Bereich der Datensicherung werden alle Einstellungen der Konfiguration gesichert. Diese können je nach Bedarf auf eine Diskette oder auf einen externen Datenträger im FAT Format gesichert werden. Zusätzlich ist als dritte Alternative möglich, Sicherungssätze anzulegen und diese herunterzuladen. Unter diesem Menüpunkt kann ebenfalls ein zuvor gesicherter Sicherungssatz wieder eingespielt werden[37, Kapitel 2.1.5].

4.1.6 Herunterfahren

Im vorletzten Punkt des Hauptmenupunktes *System* kann der IPCop heruntergefahren oder neugestartet werden. Zusätzlich besteht die Option des zeitgesteuerten Neustarts beziehungsweise Herunterfahrens[37, Kapitel 2.1.6].

4.1.7 Dank an...

Der letzte Punkt ist eine Übersicht aller am Projekt beteiligten Personen. Dazu gehören die Entwickler und die Übersetzer. Ebenfalls wird den Entwicklern der Smoothwall gedankt. Alle maßgeblich beteiligten Personen sind namentlich genannt und zum Teil über eine E-Mail Adresse kontaktierbar.

4.2 Statusmeldungen

Der nächste Hauptmenüpunkt enthält detaillierte, aufbereitete Informationen und Diagramme in den Bereichen Systemstatus und -info, Netzwerkstatus, Proxy-Diagramme und Verbindungen. Einstellungen können hier nicht vorgenommen werden, da diese Seiten ausschließlich der Information dienen.

4.2.1 Systemstatus und Diagramme

Der Benutzer erhält hier einerseits Einblick über den aktuellen Systemzustand. Dies beinhaltet etwa welche Dienste laufen, wie die Auslastung des Arbeitsspeichers und der Festplatte ist oder etwa welche Module im Kernel geladen sind. Abbildung 4.3 zeigt den Systemstatus[37, Kapitel 2.3].

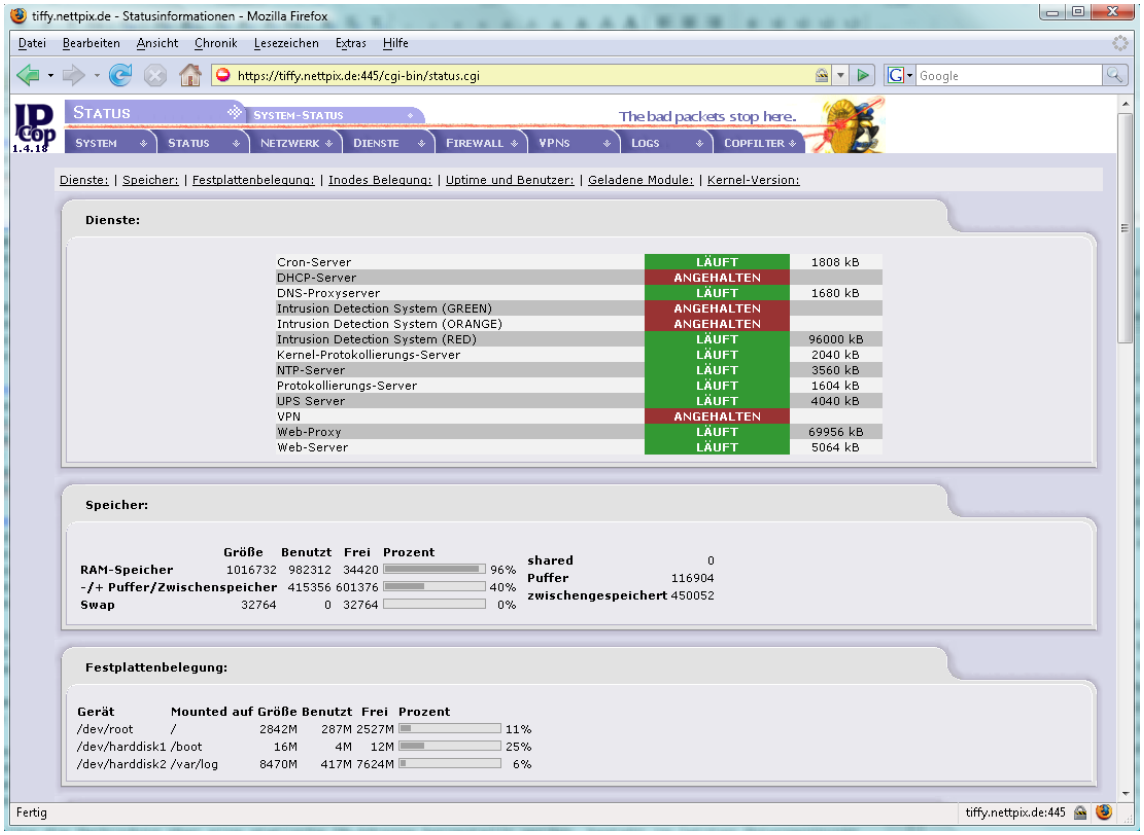

tiffy.nettpix.de - Statusinformationen - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://tiffy.nettpix.de:445/cgi-bin/status.cgi
IPCop 1.4.18
STATUS
SYSTEM-STATUS
The bad packets stop here.
SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS COPFILTER
Dienste: | Speicher: | Festplattenbelegung: | Inodes Belegung: | Uptime und Benutzer: | Geladene Module: | Kernel-Version:
Dienste:
Cron-Server LÄUFT 1808 kB
DHCP-Server ANGEHALTEN
DNS-Proxyserver LÄUFT 1680 kB
Intrusion Detection System (GREEN) ANGEHALTEN
Intrusion Detection System (ORANGE) ANGEHALTEN
Intrusion Detection System (RED) LÄUFT 96000 kB
Kernel-Protokollierungs-Server LÄUFT 2040 kB
NTP-Server LÄUFT 3560 kB
Protokollierungs-Server LÄUFT 1604 kB
UPS Server LÄUFT 4040 kB
VPN ANGEHALTEN
Web-Proxy LÄUFT 69956 kB
Web-Server LÄUFT 5064 kB
Speicher:
Größe Benutzt Frei Prozent
RAM-Speicher 1016732 982312 34420 96%
-/+ Puffer/Zwischenspeicher 415356 601376 40%
Swap 32764 0 32764 0%
shared 0
Puffer 116904
zwischengespeichert 450052
Festplattenbelegung:
Gerät Mounted auf Größe Benutzt Frei Prozent
/dev/root / 2842M 287M 2527M 11%
/dev/harddisk1 /boot 16M 4M 12M 25%
/dev/harddisk2 /var/log 8470M 417M 7624M 6%
Fertig
tiffy.nettpix.de:445

Abbildung 4.3: Screenshot der IPCop-Statusinformation

Andererseits werden hier auch Diagramme über den zeitlichen Verlauf vom Systemzustand, vom Netzwerk[37, Kapitel 2.3.4] und vom Proxydienst[37, Kapitel 2.3.5] bereit gehalten. Diese werden in der Standardeinstellung alle fünf Minuten aktualisiert und zeigen aufgeschlüsselt nach Tag, Woche, Monat und Jahr den Verlauf des jeweiligen gewählten Objekts. Eine Änderung des Intervalls ist nicht vorgesehen. Abbildung 4.4 zeigt exemplarisch ein Diagramm über den Verlauf des Datenverkehrs innerhalb einer Woche auf der grünen Schnittstelle.

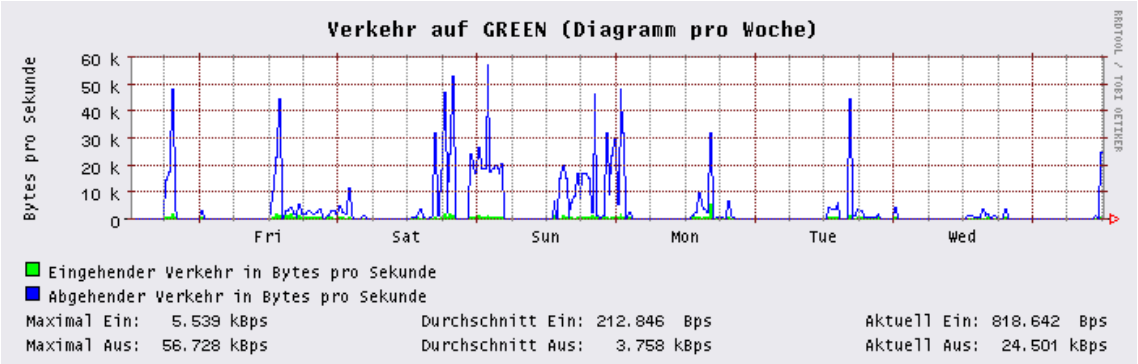


Abbildung 4.4: Screenshot des IPCop-Diagramms der grünen Schnittstelle

4.2.2 Verbindungen

Unter diesem Menü befindet sich die iptables-Verbindungsverfolgung[37, Kapitel 2.3.6]. Da auch der IPCop auf iptables und Netfilter basiert, werden alle Verbindungen zwischen den verschiedenen Geräten nach Ziel- und Quell-IP-Addresse und Ziel- und Quell-Port überwacht. Hier ist eindeutig erkennbar, welche Verbindung (von Wo nach Wo) aufgebaut wurde und zu welchem Netzwerkbereich die Verbindung gehört. Sollte dem Benutzer ein Addresse unbekannt sein, kann er auf die jeweilige IP-Adresse klicken. Er führt damit einen Reverse-DNS-Lookup durch, um das jeweilige Gerät zu identifizieren.

In Abbildung 4.5 ist der Status aktiver Verbindungen zu sehen. Deutlich erkennbar, ist hier die farbliche Trennung der verschiedenen Netzwerkbereiche. In der zweiten Zeile ist Beispielsweise die Verbindung eines Clients (IP-Adresse 192.168.150.30, grün) mit dem WebGUI des IPCops (IP-Adresse 192.168.150.1, schwarz) auf Port 445 zu sehen. Die Dritte Zeile zeigt eine Verbindung eines Clients (IP-Adresse 192.168.150.30, grün) mit dem Proxy Dienst des IPCops (IP-Adresse 192.168.150.30), erkennbar am Port 800. Die zugehörige Internetverbindung könnte Zeile acht sein. Hier stellt der IPCop eine Verbindung von der roten Schnittstelle (IP-Adresse 192.168.170.1, schwarz) mit dem Internet her (IP-Adresse 213.73.209.9, rot). In diesem Fall der Webserver der Adresse `http://www.heise.de`.

4.3 Netzwerk

Sofern der Internetzugang nicht über eine statische IP-Adresse oder über einen DHCP-Dienst bereitgestellt ist, sondern direkt über ein Modem, ISDN oder DSL-Modem, steht dem Benut-

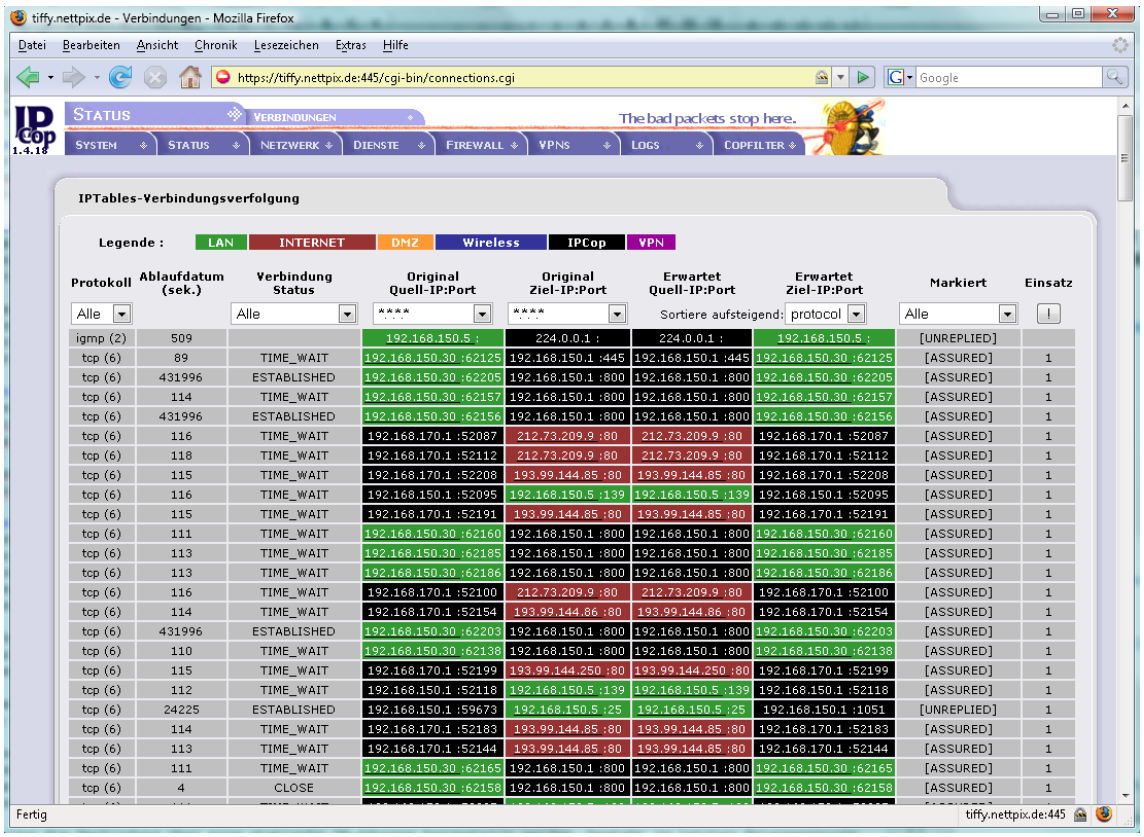


Abbildung 4.5: Screenshot der IPCop-Verbindungsverfolgung

zer in dem Menü Einwahl die Möglichkeit zur Verfügung die Einwahl der Firewall ins Internet zu konfigurieren. Dazu können fünf verschiedene Profile eingerichtet werden. Zur Option stehen dazu diverse Arten von Modems. Zusätzlich kann die Verbindung manuell, dauerhaft oder nach Bedarf (Dial on Demand) eingestellt werden[37, Kapitel 2.4].

Scheitert eine Einwahl über ein Profil, besteht zudem die Möglichkeit auf ein alternatives Profil zurückzugreifen. Dies ist zum Beispiel bei unterschiedlichen DSL-Anbietern sinnvoll, wenn ein Anbieter temporäre Probleme bei der Einwahl hat.

Damit bestimmte Modems überhaupt erst in der Lage sind eine Verbindung mit dem Internet herzustellen, kann im Punkt Hochladen[37, Kapitel 2.4.2] der jeweilige Treiber zu einem der dort aufgeführten Modems hochgeladen werden.

Wenn die Verbindung mit dem Internet über ein analoges Modem hergestellt wird, können im nächsten Punkt Modem die dazu notwendigen Kommandos wie etwa für Art der Initialisierung, der Ton- oder Pulswahl oder für das Auflegen konfiguriert werden[37, Kapitel 2.3.3].

Nach der Installation sind jedoch alle Einstellung für den Gebrauch mit den meisten Hayes-Kompatiblen Modems bereits eingetragen.

Sollte die Verbindung über eine statische IP-Adresse hergestellt werden, besteht im letzten Untermenüpunkt die Möglichkeit, in diesem Bereich weiteren vorhandenen statischen IP-Adressen Alias-Namen zu vergeben[37, Kapitel 2.4.4]. Dies ist dann notwendig, wenn im eigenen Netzwerk ein Webserver oder ein ftp-Server betrieben werden und diese über den Namen angesprochen werden sollen. Dazu ist es jedoch ebenfalls notwendig die Routingtabelle manuell anzupassen.

4.4 Dienste

Zwar ist IPCop im eigentlichen Sinn nur eine Firewall, dennoch sind einige nützliche Funktionen mit im IPCop integriert. Diese befinden sich im Menüpunkt Dienste.

4.4.1 WebProxy

IPCop wird von Haus aus direkt mit einem Web-Proxyserver ausgeliefert[37, Kapitel 2.5.1]. Dieser ist jedoch standardmäßig nicht aktiviert. Die Konfiguration des Proxyservers erreicht der Benutzer über den Punkt Dienste - Proxy. Hier kann der Proxy für die Netzwerkbereiche grün und blau aktiviert werden. Ist der Proxy aktiviert, ist eine zusätzliche Konfiguration in den Proxyeinstellungen im Browser jeden Clients zur Nutzung des Proxies notwendig. Dies ist in der Regel die Angabe der IP-Adresse der grünen Netzwerkkarte und des Port, standardmäßig Port 800. Somit kann der Benutzer entscheiden, ob er den Proxy Nutzen möchte oder nicht. Soll der Proxy in jedem Fall genutzt werden, kann er in den so genannten transparenten Modus geschaltet werden. Alle Anfragen an den Standardport 80 für HTTP-Daten werden somit an den Proxyserver umgeleitet.

Zu den weiteren Einstellungen in diesem Bereich gehört die Konfiguration des verwendeten Festplattenspeichers für den Proxy sowie die minimale und maximale Dateigröße, die in diesem Speicher abgelegt wird. Zusätzlich kann auch noch eine Dateigrößenbeschränkung konfiguriert werden, womit der Upload und/oder der Download eingeschränkt wird. Dies ist beispielsweise notwendig, wenn es ein Kontingent an Transfervolumen beim Internetdiensteanbieter gibt und dieses nicht überschritten werden soll. Der Nutzer an einem Clients wird

somit reglementiert. Feinere Reglementierungen werden erst möglich nach Installation eines weiteren AddOns wie etwa dem Advanced Proxy AddOn.

4.4.2 DNS-Server

Der im IPCop sich befindende DNS-Server erlaubt neben der Zwischenspeicherung der DNS-Abfragen ebenfalls die manuelle Zuweisung von IP-Adressen zu Hostnamen. Allerdings ist es kein echter DNS-Server, sondern ein DNS-Cache. Dieser ist Vergleichbar mit der hosts Datei unter Windows oder Linux. Es können sowohl lokale als auch öffentliche Hosts angegeben werden. Wird ein Host hinzugefügt müssen IP-Adresse, Hostname und Domainname angegeben werden. Alle erstellten Einträge können separat aktiviert oder deaktiviert werden. Eine weitere Konfiguration, etwa die Angabe übergeordneter DNS-Server ist nicht möglich.

4.4.3 DHCP-Dienst

Zur einfachen und komfortablen Netzwerkkonfiguration bietet IPCop einen DHCP-Dienst an[37, Kapitel 2.5.2]. DHCP eignet sich dazu in einem Netzwerk die Clients automatisiert im Netzwerk einzurichten. Ein weiterer Vorteil ist es, dass durch DHCP eine Mehrfachausnutzung der begrenzt zur Verfügung stehenden IP-Adressen erreicht werden kann, wobei in einem Unternehmen der hier behandelten Größe dieses Problem nicht auftreten sollte. Jedoch besteht die Gefahr, dass durch wechselnde IP-Adressen eine genaue Zuordnung zum Client nicht mehr erfolgen kann. Ebenso gibt es Programme, die sich die IP-Adresse des Clients merken zum Beispiel eine SSH-Verbindung. Eine Änderung der IP-Adresse kann dabei zu Problemen führen. Die DHCP-Konfiguration kann für das grüne und für das blaue Netzwerk separat erfolgen.

Wird DHCP eingesetzt müssen eine Start- und eine End-Adresse konfiguriert werden. Diese geben den Bereich des IP-Adresspools des DHCP-Server an. Zusätzlich können der Domänenname sowie die Primären- und Sekundären DNS-, NTP- und WINS-Server angegeben werden. Ebenfalls ist die minimale und maximale Haltezeit der Zuordnung von einem Host zu einer Adresse einstellbar. Die minimale Haltezeit gibt die Zeit an die der DHCP Server die IP-Adresse an den Host bindet. Die maximale Haltezeit gibt den Zeitraum an, in der der DHCP-Server die Anfrage des Clients in jedem Fall entgegen nimmt.

Zu diesen Angaben können noch weitere Optionen angegeben werden, etwa die Angabe eines *SMTP-Servers*, oder das *tcp-keepalive-interval*. Alle verfügbaren Optionen (98) könne hier jedoch aufgrund der Masse nicht beschrieben werden.

4.4.4 Zeitserver

Eine Möglichkeit den Clients im Netzwerk die aktuelle Uhrzeit mitzuteilen, ist die Nutzung eines Zeitserversdienstes[37, Kapitel 2.5.5]. IPCop ist mit einem solchen Zeitserver direkt ausgestattet. Dieser braucht nur noch auf einen öffentlichen Zeitserver eingerichtet werden. Dazu wird der Dienst aktiviert und ein entsprechender Zeitserver wird für den primären und sekundären Zeitserver eingetragen. Damit die Clients die Uhrzeit überhaupt empfangen können, muss die Uhrzeit schließlich noch dem Netzwerk bekannt gemacht werden. Dies geschieht, über das Programm ntpupdate. Dieses ist jedoch ungenauer als der xntp Dienst. Die Uhrzeit vom IPCop kann daher von der tatsächlichen Uhrzeit abweichen.

Schließlich wird noch die Frequenz eingestellt, wann die Uhrzeit aktualisiert werden muss. Es reicht, wenn diese alle drei Tage aktualisiert wird. Zudem kann die Uhrzeit auch jederzeit manuell aktualisiert werden.

Welcher Zeitserver genutzt wird, hängt von der lokalen Lage ab. Eine Liste mit einer Übersicht findet sich unter `http://www.ntp.org`[29].

4.4.5 Dynamisches-DNS

Im Konfigurationsmenü für Dynamisches DNS kann der Benutzer seinen bevorzugten Dynamischen DNS-Anbieter konfigurieren[37, Kapitel 2.5.3]. Sofern der Zugang zum Internet über einen ADSL-Anbieter erfolgt und der Provider nur eine dynamische IP-Adresse bereitstellt kann somit ein Zugang über einen FQDN (Full Quallified Domain Name) erfolgen. Unterstützt werden dabei alle bekannten DynDNS-Anbieter, dazu gehören unter anderem folgende, um nur einige zu nennen:

- dyndns.org
- no-ip.com
- dnspark.com
- opendns.com
- easydns.com

Die Konfiguration erfolgt, in dem der jeweilige Anbieter in einer Liste ausgewählt wird und die Zugangsdaten hinterlegt werden. Zusätzlich besteht noch die Option, ob ein zusätzlicher Proxy eingesetzt wird, und ob Wildcards im FQDN erlaubt sein sollen. Durch Klicken der Schaltfläche *Hinzufügen* wird der Dienst aktiviert. IPCop überprüft nun in regelmäßigen Abständen ob sich die IP-Adresse der Einwahl geändert hat. Die Updates können jedoch auch minimiert werden, indem vor jedem Update die IP-Adresse überprüft wird. Dies ist in der Regel für die rote Schnittstelle, dynamisch zugewiesene IP-Adresse. Befindet sich die Firewall hinter einem vor geschaltetem Router, der die Einwahl übernimmt, ist es dafür notwendig das die öffentliche IP-Adresse anhand eines externen Server geschätzt werden muss um dem Anbieter die korrekte Adresse mitzuteilen.

4.4.6 Intrusion Detection

IPCop wird direkt mit dem Intrusion Detection System (IDS) Snort ausgeliefert[37, Kapitel 2.5.7]. Ein Intrusion Detection System ist ein System, dass den Datenverkehr der durch die Firewall geht, analysiert und anhand bereits identifizierter Signaturen bösartigen Code erkennt. Das IDS ist jedoch nur ein System, dass die IP-Pakete analysiert. Es kann keine Angriffe verhindern. Dazu wäre ein Intrusion Prevention System (IPS) notwendig. Der Einsatz eines IDS Systems ist von vielen umstritten, da es zum einen Last auf der Firewall erzeugt, die keinen Nutzen bringt, und zum anderen ein IDS ebenfalls eine Sicherheitslücke bedeuten kann, falls es einen Fehler im Programmcode gibt und dieser ausgenutzt wird, um die Firewall zu kompromittieren. Dennoch ist es für den Administrator aufschlussreich zu wissen, welchen Gefahren das Netzwerk ausgeliefert ist. Der Einsatz dieses Systems liegt also im Ermessen des Administrators[2, Kapitel 6][50][51].

Da regelmäßig neue Angriffsmethoden entdeckt werden, aktualisiert Snort den Regelsatz ebenfalls fortlaufend. Diese Regeln kann das IDS im IPCop herunterladen. Dazu ist es jedoch erforderlich, dass sich der Benutzer bei der Projektseite von Snort anmeldet um einen Authorisierungscode zu erhalten. Die Nutzung der Regeln kann privat aber auch geschäftlich erfolgen. Dem Privatnutzer stehen die Regeln mit 30 Tagen Verzögerung zu Verfügung. Für aktuellere Regeln bietet Snort ein Abonnement an, welches kommerziell vermarktet wird. Auch hier ist das Herunterladen unbekannter Regeln ebenfalls eine sicherheitskritische Stelle. Die heruntergeladenen Regeln können weder analysiert noch begutachtet werden. Auch ist ein manuelles Deaktivieren einzelner Regeln nicht möglich. An dieser Stelle bleibt es wiederum dem Administrator überlassen, wie sehr er dem Anbieter der Snort-Regeln vertraut.

Die Konfiguration zur Einbruchsdetektierung Snort kann für die Netze rot, grün und blau separat aktiviert werden.

4.4.7 Traffic Shaping

Traffic Shaping ist eine Möglichkeit, den Datenstrom bei der Übertragung zu optimieren[37, Kapitel 2.5.7]. Bei diesem Verfahren werden Regeln aufgestellt welche Daten bevorzugt behandelt werden, und welche Daten verzögert zum Client ausgeliefert werden, sofern höher priorisierte Daten anstehen. In der Standardkonfiguration ist IPCop mit dem Traffic Shaper WonderShaper ausgestattet. Dieser ist auf die Minimierung der Ping-Latenzzeiten ausgerichtet, und stellt sicher, dass für den jeweiligen konfigurierten Dienst eine genügend hohe Bandbreite zur Verfügung steht.

Die Konfiguation im IPCop ist eher minimalistisch gehalten. Dem Benutzer muss zum einen die maximal verfügbare Up- und Downloadrate bekannt sein. Diese werden in die Konfigurationsseite des IPCop eingetragen. Danach werden die Dienste konfiguriert, die hoch bzw. niedrig priorisiert werden sollen.

4.5 Firewall

Im Menüpunkt Firewall werden Regeln für die im Netzwerk angebotene Dienste hinterlegt. Diese sind in verschiedene Bereiche unterteilt, je nach Ziel des zu erreichenden Dienstes.

4.5.1 Port-Forwarding

Einer der wichtigsten Funktionen des IPCop ist das Port-Forwarding[37, Kapitel 2.6.3]. Dieser Punkt befindet sich im Menü Firewall. Hier werden die Regeln der erlaubten Verbindungen definiert. So sind nach Installation des IPCop erst einmal alle Verbindungen von außerhalb zum inneren Netzwerk gesperrt. Über die Regeln kann nun für jeden beliebigen Dienst ein Loch in der Firewall erstellt werden. Gibt es etwa einen Webserver oder einen E-Mail-Server im internen Netz muss der jeweilige Port und der entsprechende Rechner in einer Regel festgehalten werden. Dazu wird das entsprechende Protokoll ausgewählt, der Quell- und Zielport

angegeben und eine entsprechende Ziel-Adresse. Ein Bemerkungstext zur einfacheren Identifizierung der Regel kann ebenfalls angegeben werden.

4.5.2 Externer Zugang

Um bestimmte Dienste auf der Firewall auch von außerhalb des internen Netzes zu erreichen, gibt es die Möglichkeit, auch dafür bestimmte Regeln zu definieren[37, Kapitel 2.6.4]. Es ist beispielsweise möglich, den IPCop über eine SSH Verbindung (für den IPCop Port 222) fernzusteuern. Genauso ist es möglich, das Webfrontend des IPCop von extern über eine hier definierte Regel zum Port 445 erreichbar zu machen. Es ist jedoch nicht empfehlenswert, die erstellen Regeln dauerhaft zu aktivieren. Vielmehr sollten alle nicht erstellten Regeln deaktiviert bleiben und nur nach Bedarf aktiviert werden, um mögliche Angriffspunkte zu vermeiden.

4.5.3 DMZ-Schlupflöcher

Eine weitere Konfigurationsseite zur Regelerstellung verbirgt sich unter der Option DMZ-Schlupflöcher[37, Kapitel 2.6.5]. Sofern eine DMZ im Netzwerk eingesetzt wird, müssen für die dort hinterlegten Dienste ebenfalls Regeln eingerichtet werden. Die Konfiguration gestaltet sich hier ähnlich wie bei den beiden Punkten zuvor. Es müssen Protokoll, Quell- und Zielnetz sowie Port angegeben um dem Dienst Zugriff auf das interne Netz zu gewähren.

4.5.4 Firewall Optionen

Unter diesem Punkt verbirgt sich die Einstellung zum Deaktivieren des ICMP Ping[37, Kapitel 2.6.7]. Dieser kann entweder für alle oder nur für die rote Schnittstelle konfiguriert werden. Jedoch ist es nicht ratsam diese Einstellung generell für alle ICMP Pakete durchzuführen, da es sinnvolle und weniger sinnvolle Pakete gibt. Zumal ein Verstecken des IPCop nicht möglich ist, da ein nicht antwortender Router immer noch existiert und dies durch seine ausbleibende Antwort dem anfragenden Client kommuniziert.

4.6 VPN

IPCop eignet sich ebenfalls dazu, zwei von einander getrennte Netzwerke über ein drittes Netzwerk hinweg, miteinander zu Verbinden. Alle Daten aus dem ersten Netzwerk lassen sich, mit entsprechender Berechtigung vorausgesetzt, über die VPN-Verbindung erreichen und umgekehrt. Die Daten die zwischen diesen beiden Netzwerken ausgetauscht werden sind verschlüsselt, könne also nicht von anderen die sich im dritten Netzwerk befinden eingesehen werden[37, Kapitel 2.7].

IPCop unterstützt dabei die Verbindung zweier IPCops untereinander, aber auch andere VPN-Produkte, die auf das verwendete Protokoll IPSec aufbauen. Unterschieden werden im IPCop zwischen Netz-zu-Netz- und Host-zu-Netz-Verbindungen. Bei der Methode Netz-zu-Netz können mindestens zwei private Netze miteinander Verbunden werden. Die Methode Host-zu-Netz wird Benutzt, um von einem externen Client eine Verbindung mit dem privaten Netz herzustellen. Dies kann ein Notebook sein, das sich über eine Wählverbindung mit dem Internet verbunden hat.

Bevor VPN genutzt werden kann, muss sich der Administrator für eine Authentifizierungsmethode entscheiden[37, Kapitel 2.7.2]. Zur Auswahl stehen dazu die Nutzung eines Pre-Shared Keys und die zertifikatbasierte Authentifizierung. Mit einem Pre-shared Key, was einem Passwort gleich kommt, lässt sich ein VPN-Netzwerk schnell aufbauen. Allerdings eignet sich diese Methode nicht für die Option Host-zu-Netz, da der Pre-shared Key bei allen Hosts der gleiche ist.

Eindeutig sicherer ist die Verwendung von X.509 Zertifikaten. Ein X.509 Zertifikate enthält in der Regel einen privaten und einen öffentlichen Schlüssel, Passwörter sowie Informationen über die zu zertifizierende Funktionseinheit. Das Zertifikate wird von einer vertrauenswürdigen Stelle ausgestellt und kann von einer Zertifizierungsstelle auf Gültigkeit überprüft werden. Der IPCop ist selbst eine solche Zertifizierungsstelle und kann Zertifikate erzeugen. Er kann aber auch durch eine andere Zertifizierungsstelle ausgestellte Zertifikate nutzen.

Um VPN einzurichten sind vorerst globale Einstellungen notwendig. Dazu gehört die Angabe des Hostnames des IPCop beziehungsweise die öffentliche IP-Adresse des IPCops. Wird ein dynamisch DNS benutzt ist es empfehlenswert, eine Verzögerung mit anzugeben, wann das VPN-Netzwerk gestartet werden soll. Ebenso kann angegeben werden, dass VPN neugestartet wird, sobald sich die dynamische IP-Adresse geändert hat.

Im Verbindungsstatus können bestehende VPN-Verbindungen kontrolliert und überwacht werden sowie neue hinzugefügt werden. Im Bereich der Zertifizierungsstellen können ein Root- und Host-Zertifikat erstellt werden. Hier kann ebenfalls ein bereits bestehendes Zertifikat auf den IPCop hochgeladen werden.

Um nun eine VPN-Verbindung zu erstellen, wird der Assistent zur Einrichtung durch Klicken auf den Schalter *Hinzufügen* gestartet. Dort wird im ersten Schritt der Verbindungstyp, Netz-zu-Netz oder Host-zu-Netz ausgewählt[37, Kapitel 2.7.4.2]. Im nächsten Schritt werden nun die Verbindungsparameter angegeben. Diese sind der Name der Verbindung zur Kennzeichnung, die Host-IP-Adresse und Subnetz, sowie die erlaubte Remote-Adresse und Subnetz. Zusätzlich kann angegeben werden was mit der Verbindung geschieht, sobald der Remote-Host nicht mehr erreichbar ist (Dead Peer Detection).

Danach erfolgt die Angabe der Authentifizierung. Diese kann, wie bereits angegeben, über einen Pre-Shared Key erfolgen, oder über ein Zertifikat.

Da die Einrichtung eins VPNs jedoch problematisch sein kann, das Thema VPN sehr komplex ist und hier nicht alle Fälle abgebildet werden können, wird an dieser Stelle zur weiteren Einrichtung eines VPNs auf dem IPCop auf die Seite von Eckart Gutzeit[21] verwiesen.

5 Weitere Funktionen und Dienste - AddOns

IPCop ist zwar bereits in der Grundausstattung mit vielen sinnvollen und nützlichen Funktionen ausgestattet, jedoch sind diese Funktionen entweder für die eingesetzten Bedürfnisse nicht ausreichend, teilweise in einem eingeschränktem Funktionsumfang oder sie fehlen ganz. Andererseits lassen sich mit Addons Funktionen auf den IPCop integrieren, die zwar streng genommen nicht auf einer Firewall laufen sollten, in Abwägung zwischen Sicherheit und Nutzen dem Benutzer zusätzliche Möglichkeiten und Optionen bereitstellen.

Ein Beispiel für eine fehlende Funktion ist die gänzliche Öffnung des Datenverkehrs vom internen Netzwerk nach außen. Durch den Einsatz des IPCops gelangt zwar kein ungewollter Datenverkehr mehr ins interne Netz oder in die DMZ (nur mittels Port-Forwarding oder Pinholes), aber sämtlicher Verkehr auf allen Ports kann ungehindert ins Internet gelangen. Wie bereits im ersten Kapitel erwähnt, erfolgen die meisten Angriffe innerhalb des Netzwerks und nicht von außerhalb. Ist also ein Trojaner auf einem internen Rechner installiert, könnte dieser ungehindert (auch unbemerkt) wichtige Daten einem Angreifer liefern. Das Tool zur Gegenmaßnahme nennt sich in diesem Fall BOT, oder auch BlockOutTraffic genannt.

Dieses AddOn und weitere nützliche Funktionen und Dienste sind nachfolgend beschrieben und werden in einer Standardkonfiguration vorgestellt. Da es jedoch eine Vielzahl von AddOns gibt und diese hier nicht alle behandelt werden können, wird an dieser Stelle auf die Seite `http://www.ipcopaddons.org` verwiesen.

In der Tabelle 5.1 befindet sich eine übersichtliche Darstellung ausgewählter AddOns. Diese werden nachfolgend vorgestellt.

Tabelle 5.1: Übersicht AddOns

AddOn	Funktion	Download
QoS - Quality of Servie (2.6.6.1)	AddOn zur Bandbreitenregelung	http://www.mhaddons.tk/
BOT - BlockOut Traffic (3.0.0)	GUI basierte Erstellung von Firewallregeln zur Kontrolle aller Verbindung durch die Firewall.	http://blockouttraffic.de/
Advanced Proxy (2.1.7)	Umfangreicher Proxy mit Möglichkeit zur Authentifizierung	http://www.advproxy.net/
Update Accelerator (2.0.0)	Proxybasierte Zwischenspeicherung von diversen Softwareaktualisierungsseiten	http://www.mhaddons.tk/
Calamaris (2.1.1)	Proxylogauswertung des Advanced Proxys	http://www.advproxy.net/calamaris/
URL-Filter (1.9.1)	Umfangreicher Internetinhaltsfilter	http://www.urlfilter.net/
Copfilter (0.84beta3a)	Umfangreiche AddOn-Sammlung zur Virenprüfung und SPAM-Bekämpfung von E-Mails und Internet	http://www.mhaddons.tk/
Ucarp - High availability AddOn (2.3)	AddOn zur Bereitstellung einer hoch verfügbaren Internetverbindung	http://www.mhaddons.tk/
Webalizer (1.8)	Auswertung der Squid Logfiles	http://www.h-loit.de/
Line Test (4.4)	Verbindungsüberprüfung und automatische Neueinwahl durch unterschiedliche Profile	http://www.h-loit.de/
GUI-Ports (1.6.2)	Erlaubt die Modifikation der Standard-Port des WebGUIs	http://www.h-loit.de/
UPS (0.5.7)	Einbindung einer Unterbrechungsfreien Stromversorgung (Wartung und Log)	http://www.h-loit.de/
SystemInfo (2.4.5)	Zeigt weitere Systeminformationen im WebGUI an	http://www.ipadd.de/binary.html
SnortALog (2.4.0)	Detaillierte Auswertung und Berichtserstellung des Snortlogs	http://www.mhaddons.tk/
FirewallLogs (1.1.1)	Auswertung der Firewalllogdatei mit Filterung nach Quell-IP-Adresse und Ziel-Port	http://www.mhaddons.tk/
RootkitHunter (1.2.9)	Ermöglicht die Suche nach einem bekannten Rootkit auf dem IPCop	http://www.mhaddons.tk/
Coptime (0.4.0)	AddOn zur Teilnahme an einer Uptime Datenbank.	http://www.coptime.de/

5.1 Quality of Service

Zwar erlaubt der IPCop bereits eine gewisse Steuerung der Bandbreite, jedoch ist das eingebaute Traffic Shaping in der die Konfiguration sehr begrenzt. Das Quality of Service AddOn wird zur ebenfalls zur Bandbreitenregulierung eingesetzt. Bandbreitenregulierung ist sinnvoll, wo zu wenig Bandbreite vorhanden ist oder eine zu hohe Teilnehmerzahl sich die Bandbreite teilen muss. Zum Tragen kommen hier unterschiedliche Gründe. Ein ADSL-Zugang hat eine geringe Uplink-Bandbreite. Dadurch entstehen Staus im Datenstrom, was zu Verlusten von Paketen führt. Auch gibt es höhere Latenzen bei interaktiven Diensten, wie SSH und/oder Voip. Die Aufgabe vom QoS ist es die Pakete zu sortieren um so die Leitung besser auszulasten. Es stehen zwei AddOns zur Verfügung. QoS basierend auf der Methode Hierarchical Fair Service Curve (HFSC) und QoS NG basierend auf Hierarchical Token-Bucket (HTB).

> Während HTB hauptsächlich Token-Bucket Filter (TBF) in eine hierarchische Struktur gliedert und dabei die wesentlichen Eigenschaften eines TBFs beibehält, erlaubt der HFSC Algorithmus neben der proportionalen Aufteilung der Bandbreite zudem noch die Vergabe und Kontrolle von Latenzzeiten. Dies ermöglicht eine bessere und effizientere Nutzung der Leitung in Szenarien, in denen sowohl bandbreiten-intensive Daten-Dienste und als auch interaktive Dienste sich eine Leitung teilen[28].

Ein QoS wird in einem Netzwerk mit nur einem Client, besser gesagt mit einem einzelnen Download, keinen Vorteil haben. Im Gegenteil, der Download wird sogar langsamer durch die Sortierung der Pakete. Allerdings sorgt das QoS dafür, das in einem Netzwerk in dem sich viele Clients die Verbindung teilen, die einzelnen Verbinden sich nicht stören oder sogar behindern. QoS sorgt dafür, das zwei Benutzer die an einer 1Mbit-Datenleitung hängen jeweils beide mindestens 500Kbit Bandbreite bekommen. Benutzt nur einer von beiden die Verbindung bekommt derjenige die gesamte Bandbreite. Abbildung 5.1 verdeutlicht diese Funktionsweise[28].

Installation Bevor das AddOn installiert werden kann, ist es erforderlich einen layer7 Filter zu installieren. Dieser integriert sich in den Linux-Kernel und benutzt reguläre Ausdrücke um die Netzwerkprotokolle zu identifizieren. Der layer7 Filter und das AddOn werden zusammen auf den IPCop in ein temporäres Verzeichnis kopiert. Es erfolgt zuerst die Installation des layer7 Filter. Dieser wird durch den Befehl *tar xvfj IPCop-1.4.15-kernel.tar.bz2 -C /* installiert. Danach erfolgt der Befehl *touch /var/run/need-depmod-ùname -r`* sowie der Neustart

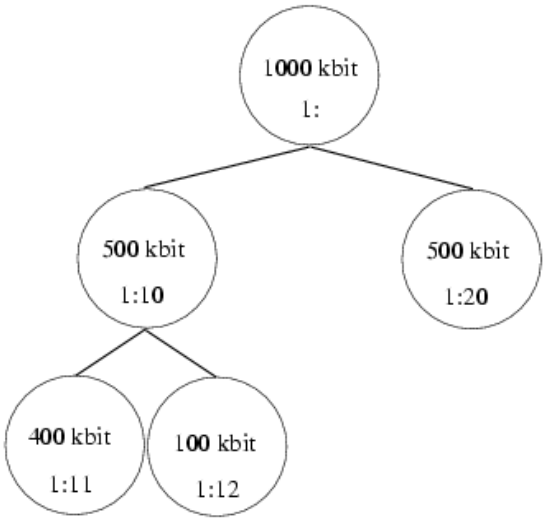


Abbildung 5.1: QoS Funktionsweise[28]

des IPCops. Nach erfolgtem Neustart wird das QoS AddOn ebenfalls mit tar entpackt und kann durch Eingabe des Befehls *./install* im durch tar erstellten Verzeichnis installiert werden. QoS wird als eigener Menüpunkt im Menü *Dienste* eingerichtet[55].

Konfiguration Bei der Einrichtung des QoS werden Klassen erstellt. Jede Schnittstelle hat eine eigene root-Klasse in der die maximale Bandbreite angegeben wird. Danach werden weitere Unterklassen definiert. Dies ist je nach Anwendungsfall sehr unterschiedlich. In diesem Beispiel werden drei Klassen definiert. Eine schnelle, eine langsame und eine normale Klasse. Tabelle 5.2 zeigt die Klassen detailliert auf.

Tabelle 5.2: Übersicht Klassen

Klasse	Priorität	Verzögerung	min Bandbreite	max Bandbreite
100	4	50 ms	100 kbps	keine Begrenzung
101	1	40 ms	30 kbps	keine Begrenzung
102	7	100 ms	0 kbit	keine Begrenzung

Nach dem die Unterklassen definiert sind, können in den Klassen die zu steuernden Pakete definiert werden. Dazu gibt es zwei Möglichkeiten, die Nutzung des layer7 Filter und die Verwendung einer Regel die über den Port gesteuert wird. Dies ist notwendig, da der layer7 Filter nicht immer zuverlässig alle Protokolle erkennt. Bei beiden Methoden kann zudem eine

Quell- und/oder Zieladresse angegeben werden, um die Regel zu beschränken. Ohne Angabe wird die erstelle Regel auf jeden Host angewendet.

Nach der Erstellung der Regeln kann das QoS gestartet werden. In jedem Fall ist es jedoch ratsam sich vor der Einrichtung zu Überlegen, welcher Datenverkehr im Netzwerk vorkommt und wie dieser gesteuert werden soll. Daraufhin werden die Klassen erstellt und anschließend die Regeln definiert[58].

5.2 BlockOutTraffic

Wie in Abbildung 3.2 gezeigt, sind nicht alle Verbindungswege gesperrt. BlockOutTraffic (BOT) ist ein Addon, welches diese Verbindungen nachträglich blockiert. Verbindungen sind nur noch dann erlaubt, wenn dazu eine entsprechende Regel erstellt wurde. Durch dieses AddOn wird die Firewall wesentlich sicherer, da nur noch gewollte Verbindungen durchgelassen werden, was jedoch einen erheblicheren Planungsaufwand bei der Konfiguration bedeutet. Zudem wird dadurch eine flexiblere Kontrolle der Verbindungen zur Firewall und durch die Firewall möglich. Die Regeln werden über das Webfrontend des IPCops erstellt und verwaltet[55]. Abbildung 5.2 zeigt die auf einem IPCop bereits erstellten Regeln.

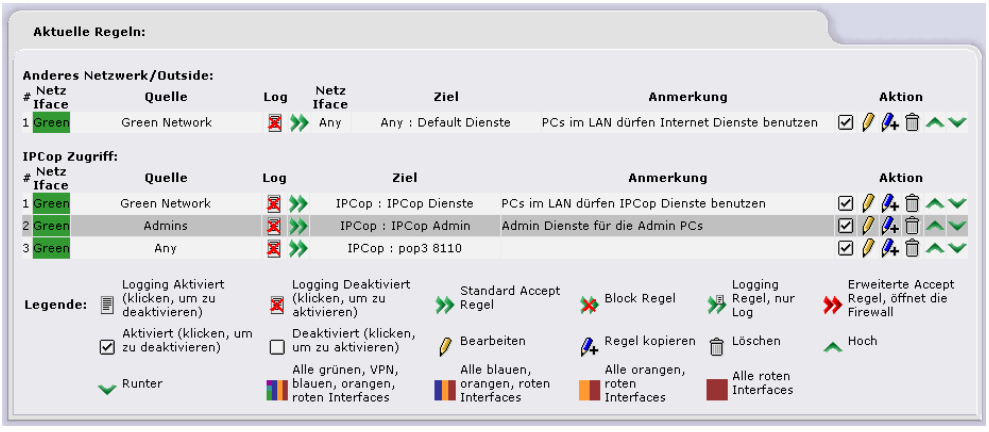

Aktuelle Regeln:
Anderes Netzwerk/Outside:
Netz Iface Quelle Log Netz Iface Ziel Anmerkung Aktion
1 Green Green Network Any Any : Default Dienste PCs im LAN dürfen Internet Dienste benutzen
IPCop Zugriff:
Netz Iface Quelle Log Ziel Anmerkung Aktion
1 Green Green Network IPCop : IPCop Dienste PCs im LAN dürfen IPCop Dienste benutzen
2 Green Admins IPCop : IPCop Admin Admin Dienste für die Admin PCs
3 Green Any IPCop : pop3 8110
Legende:
Logging Aktiviert (klicken, um zu deaktivieren)
Logging Deaktiviert (klicken, um zu aktivieren)
Standard Accept Regel
Block Regel
Logging Regel, nur Log
Erweiterte Accept Regel, öffnet die Firewall
Aktiviert (klicken, um zu deaktivieren)
Deaktiviert (klicken, um zu aktivieren)
Bearbeiten
Regel kopieren
Löschen
Hoch
Runter
Alle grünen, VPN, blauen, orangen, roten Interfaces
Alle blauen, orangen, roten Interfaces
Alle orangen, roten Interfaces
Alle roten Interfaces

Abbildung 5.2: Screenshot BOT Regeln in einem IPCop

Installation Die Installation erfolgt durch Übertragen des Pakets in ein temporäres Verzeichnis auf dem IPCop. Dieses wird mit tar entpackt. Anschließend wird die Installation

durch Eingabe des Befehls *./setup* gestartet. Die Installation läuft automatisiert und ohne weitere Nachfragen ab. Nach der Installation befinden sich zwei zusätzliche Menüpunkte im Firewallmenü des IPCop-WebGUIs. Zum Einen der Punkt für die generellen Einstellungen zu BOT, zum anderen der Menüpunkt für die erweiterte Konfiguration[58].

Konfiguration Bevor das AddOn aktiviert werden kann, ist es zwingend erforderlich, einige Einstellungen vorzunehmen. Werden diese nicht vorgenommen und das AddOn gestartet, sperrt sich der Benutzer aus und hat keine reguläre Möglichkeit sich erneut mit dem IPCop zu verbinden. In einem solchen Fall hilft nur noch die Anmeldung am IPCop selbst und das Zurücksetzen der durch BOT erstellten iptables Regeln durch die Eingabe des Befehls *iptables -F BOT_INPUT*[56]. Die Grundkonfiguration erreicht der Benutzer im Menüpunkt *Block Outgoing Traffic* nach dem Klicken auf den Schalter *Einstellungen*.

Die erste Einstellung die vorgenommen wird, ist das Eintragen der Client-MAC-Adresse sowie des HTTPS Ports des IPCop WebGUIS, mit der sich der Benutzer am IPCop anmeldet. Dadurch wird eine Standard-Zugriffsregel erstellt, die nur noch die Anmeldung von diesem Client am IPCop zur Administration erlaubt. Dies ist bereits eine deutliche Erhöhung der Sicherheit im internen Netz.

Die nächste Option, *Verbindungs Status*, ist zuständig die Pakete durch zulassen, die zu einer bereits bestehenden oder angeforderten Verbindung gehören. Sind Port-Weiterleitung eingerichtet, etwa wegen einem Webserver im internen Netzwerk, muss diese Option aktiviert werden.

In der Anfangsphase, aber auch später ist es nützlich, wenn Pakete geloggt werden die auf keine der erstellen Regeln passen. Durch Aktivieren der Option für Logging wird diese Funktion ebenfalls eingeschaltet. Auch kann die Methode des Blockverhaltens angegeben werden. Dies ist entweder Reject, also ablehnen oder Drop, verwerfen.

Eine weiter Einstellung aktiviert den erweiterten Modus. Diese sollte jedoch nur von erfahrenen Administratoren aktiviert werden, da in der erweiterten Konfiguration die gesamte Firewall geöffnet werden kann. Die Maske wird nun mit Speichern verlassen.

Nach der Grundkonfiguration können die ersten Regeln erstellt werden. Dazu sollten jedoch vorher benutzerdefinierte Dienste angelegt werden die später in den Dienste Gruppen oder

BOT Regeln ausgewählt werden können. Es bietet sich an drei Dienste zu konfigurieren. *IPCop SSH* für den Zugang über eine SSH Verbindung, *IPCop hhtps* für den Zugang zum WebGUI über andere Clients als die des Admins und den Dienst *IPCop Proxy* für die Benutzung des Proxys. Die Dienste werden im Menü *Erweiterte BOT Konfig* hinzugefügt. Als nächstes können nun verschiedene Gruppen definiert werden abhängig davon was erlaubt werden soll. Es wird davon ausgegangen, das den Clients erlaubt werden soll E-Mail zu nutzen und zu surfen, die Dienste DNS, DHCP und NTP auf dem IPCop zu benutzen sowie zusätzlichen Clients die Administration des IPCop über SSH und WebGUI zu erlauben. Dazu können drei Gruppen angelegt werden: *Default Dienste*, *IPCop Admin* und *IPCop Dienste*. In jeder Gruppe können nun die entsprechenden Ports angelegt werden. Etwa in der Gruppe Default Dienste die Ports für SMTP, IMAP und POP3, in der IPCop Admin Gruppe die bereits erstellten Dienste *IPCop SSH* und *IPCop https* und in der IPCop Dienste Gruppe die Dienste *Domain* für das DNS auf dem Cop, die Dienste *bootpc* und *bootps* für den DHCP-Dienst, *ntp* für den Zeitserver und den bereits erstellten Dienst *IPCop Proxy* für die Nutzung des Proxyservers.

Nach selbigem Schema können selbstverständlich auch weitere Dienste und Gruppen definiert werden. Ganz nach den Bedürfnissen der eigenen Netzwerkstruktur. Nachdem alle Gruppen und Dienste angelegt sind, können nun die Regeln erstellt werden. Dies geschieht wiederum unter dem Menüpunkt *Block Outgoing Traffic*. Die erste Regel die angelegt wird, erlaubt den Clients Zugriff auf die IPCop Dienste. Dazu wird erst die Quelle gewählt, einmal das grüne Interface und zusätzlich das grüne Netzwerk. Danach wird das Ziel angegeben. In diesem Fall ist es einmal der IPCop Zugriff sowie der Benutzter Dienst, der zuvor eingerichteten Gruppe *IPCop Dienste*. Die Regel muss aktiviert werden und kann zusätzlich bei einem Treffer auch einen Logeintrag erzeugen. Zusätzlich kann ein Zeitrahmen definiert werden in dem diese Regel gilt. In diesem Fall ist das nicht erforderlich. Nach klick auf den Schalter *Weiter* gelangt der Benutzer auf eine Übersichtsseite in der bei zusätzlich vorhandenen Regeln die Reihenfolge der Regeln beeinflusst werden kann. Durch einen Klick auf den Schalter *Speichern* wird die Regel übernommen.

Auf die gleiche Weise wird eine Regel für die Benutzung der *Default Dienste* erstellt. Die Quelle ist hier wieder das grüne Interface und das grüne Netzwerk. Ziel ist nun jedoch die Option *Anderes Netzwerk/Outside* sowie *Any* in der Option *Standard Netzwerke*. Auch hier muss die Option *Benutze Dienste* aktiviert werden und die zuvor erstellte Gruppe *IPCop-Dienste* ausgewählt werden. Nach Einstellung aller Optionen kann diese Regel ebenfalls aktiviert und gespeichert werden.

Nun fehlt noch die Regel für den Administrationszugriff mehrere Clients auf dem IPCop. Dazu

müssen zunächst in der erweiterten BOT Konfiguration in den Adresseinstellungen diejenigen Adressen (MAC- oder IP-Adressen) angegeben werden die Zugriff bekommen sollen. Danach können diese ebenfalls, wie die zuvor definierten Dienste, zu einer Gruppe zusammengefasst werden. Danach kann die passende Regel erstellt werden. Die Quelle ist wiederum das grüne Interface. Diesmal wird zusätzlich die zuvor erstellte Adress-Gruppe *Admins* ausgewählt. Das Ziel ist der *IPCop Zugriff* sowie der Benutzte Dienst *IPCop-Admins*.

Nachdem alle Regeln erstellt sind, kann das AddOn aktiviert werden. Sofort nach der Aktivierung sind die Regeln aktiv, und es gelangt nur noch der Traffic durch die Firewall der mit den Regeln definiert wurde[57].

5.3 Advanced Proxy

Da die bestehende Proxyfunktionalität im IPCop stark eingeschränkt ist, bis auf den verwendeten Speicherplatz und die Objektgröße ist nichts weiter einstellbar, besteht die Möglichkeit den Advanced Proxy als Erweiterung zu installieren. Dieses Proxy AddOn, welches ebenfalls den bestehenden Squid Proxy benutzt, ist ein mächtiges Paket welches dem Administrator weitere Funktionalitäten und Leistungsmerkmale bereitstellt. Eine auf den Advanced Proxy basierende Funktion ist die Class Room Extension, welche jedoch in dieser Arbeit nicht besprochen wird. Sie ist eher für Bildungseinrichtungen interessant und kann zur Einrichtung von Gruppen, den so genannten Klassenräumen, genutzt werden. Diese können dann gezielt über ein Webfrontend verwaltet werden[43].

Neben der Basisfunktionalität den Datenverkehr zu cachen, besteht eine ausführliche Netzwerkbasierte Zugriffskontrolle. Eine Einschränkung auf einen Zeitraum ist ebenso möglich wie die Beschränkung der Transfergrößen und Bandbreite. Der Advanced Proxy bietet darüber hinaus an bestimmte MIME-Typen zu sperren oder nur eine Auswahl bekannter Browser zu erlauben.

Ein weiterer wesentlicher Vorteil des Advanced Proxy AddOns besteht in der Authentifizierung. Darüber wird gewährleistet, dass es nur einem bestimmten Benutzerkreis gestattet ist den Proxy zu benutzen, oder aber gewissen Personen die Benutzung zu verweigeren. Der Proxy unterstützt dazu die Methoden lokale Authentifizierung, Authentifizierung über einen Identd Daemon oder Dienst, Windows Authentication, LDAP Authentication und RADIUS.

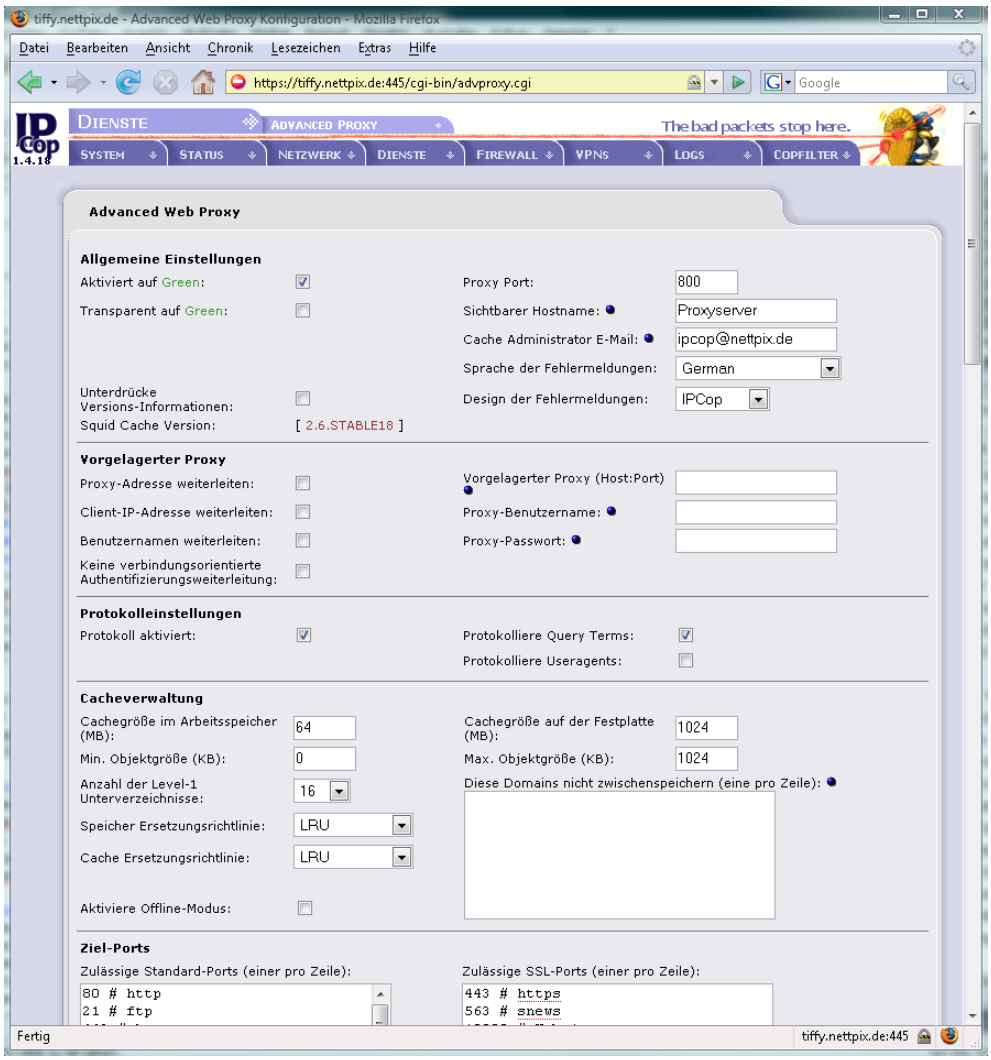


Abbildung 5.3: Screenshot Konfigurationsmaske Advanced Proxy

Der Entwickler hat zu diesen Funktionen noch den Update Accelerator entwickelt. Dieser ist ein separater Cache in dem Updates für gängige Software bereitgehalten werden, etwa Microsoft Windows Updates oder Aktualisierungen für gängige Virenscanner (Avast, Symantec, Trend Micro).

Installation Die Installation wird durchgeführt in dem das Paket von der Projektseite des AddOns heruntergeladen wird, und diese auf den IPCop in ein temporäres Verzeichnis kopiert wird. Dort wird es mittels tar entpackt. Die Installation wird darauf im entpackten Verzeichnis durch Eingabe von *./install* gestartet. Die Installation läuft automatisiert ab. Die Installation ändert den vorhanden Menüeintrag des bestehenden IPCop-Proxys in seinen Eigenen. Der alte

Eintrag wird nicht mehr benötigt[42].

Konfiguration In der Einstellungsmaske für den Advanced Proxy, siehe Abbildung 5.3, werden zunächst die allgemeinen Einstellungen konfiguriert. Dazu gehört die Aktivierung des Proxys, der Port unter dessen der Proxy erreichbar ist, ob der Proxyserver im transparenten Modus läuft und in welcher Sprache und in welchem Design die Fehlermeldungen des Proxies dargestellt werden. Der Proxyserver darf nicht im transparenten Modus laufen wenn eine der Authentifizierungsmethoden genutzt werden soll.

Danach erfolgt die Konfiguration bei Nutzung eines vorgelagerten Proxyservers[41]. Dieser kann nützlich sein bei Verwendung eines weiteren Proxyservers um einen zusätzlichen ContentFilter zu integrieren wie etwa das hier nicht besprochenen AddOn DansGuardian oder Privoxy aus dem AddOn Copfilter. Dazu muss jedoch der Host und Port des Proxies mit angegeben werden. Ist einen Authentifizierung erforderlich wird diese ebenfalls hier hinterlegt.

Danach erfolgt die Einstellung zur Protokollierung. Dies kann aktiviert und deaktiviert werden. Zudem können bei dynamischen Abfragen die Query Terms mit protokolliert werden. Ebenso kann auch der UserAgent mit protokolliert werden. Dieser erscheint jedoch nicht im GUI sondern nur im Verzeichnis */var/log/squid/useragent.log*. Es sollte auch nur zur Fehlersuche aktiviert werden, das diese Datei ebenfalls sehr groß werden kann.

Die Einstellungen der Cacheverwaltung beeinflussen das Verhalten des Caches. Es lassen sich wie im Standard IPCop Proxy die Cachegröße sowie die kleinste und größte zu cachende Dateigröße angeben. Ein weiterer Wert ist die Angabe des zu nutzenden Arbeitsspeichers. Der hier angegebenen Wert wird für negativ gecachte und In-Transit-Objekte verwendet.

Der nächste Wert beeinflusst die Anzahl der Level-1 Unterverzeichnisse des Festplattencaches. Dieser ist in der Voreinstellung auf 16 eingestellt. Dies entspricht 4.096 Verzeichnissen. Der Wert kann auf 256 erhöht werden, was einer Gesamtzahl von 65.536 Verzeichnissen entspricht. Dieser Wert sollte nur erhöht werden wenn es erforderlich ist, da der Startprozess dadurch signifikant verzögert werden kann.

Die nächsten beiden Parameter beeinflussen die Ersetzungsrichtlinie im Speicher und im Festplattencache. Es stehen die Optionen wie in Tabelle 5.3 dargestellt zur Auswahl.

Als nächstes kann angegeben werden, das bestimmte Domains nicht in den Cache mit aufgenommen werden, sondern immer direkt aus dem Internet geladen werden. Dies ist besonders bei Suchmaschinen oder sich häufig ändernden Seiten interessant.

Tabelle 5.3: Speicher/Cache Ersetzungsrichtlinie[41]

Methode	**Funktion**	**Beschreibung**
LRU	Squids ursprüngliche, listenbasierte Last Recently Used-Richtlinie	Die LRU-Richtlinie behält kürzlich referenzierte Objekte, d.h. sie ersetzt das Objekt, auf das am längsten nicht zugegriffen wurde
heap LRU	Last Recently Used policy basierend auf einen heap	Arbeitet wie LRU, verwendet aber stattdessen einen Heap
heap LFUDA	Least Frequently Used mit Dynamic Aging	Die heap LFUDA-Richtlinie (Least Frequently Used with Dynamic Aging) behält häufig angefragte Objekte ungeachtet ihrer Größe im Cache und optimiert deswegen die Byte-Trefferrate auf Kosten der gesamten Trefferrate, da ein einziges großes Objekt möglicherweise das Caching von mehreren kleineren, nicht so häufig angefragten Dateien verhindert.
heap GDSF	Greedy-Dual Size Frequency	Die heap GDSF-Richtlinie optimiert die Rate der gefundenen Objekte dadurch, dass kleinere, öfter angefragte Objekte im Cache gehalten werden. Sie erzielt jedoch eine geringere Byte-Trefferrate als LFUDA, dadurch, dass sie größere (möglicherweise öfter angefragte) Objekte aus dem Speicher entfernt.

Im nächsten Bereich werden die erlaubten Ziel-Ports konfiguriert, die über den Advanced Proxy laufen sollen. Sie sind getrennt nach Standard HTTP und SSL-verschlüsselten-Anfragen aufgeführt.

Danach folgt die Definition der netzwerkbasierten Zugriffskontrolle. Es können hier erlaubte Subnetze angegeben werden, falls mehrere verwendet werden ein pro Zeile. Ebenso erfolgt hier die Einstellung welche IP- oder MAC-Adressen von regelbasierten Einschränkungen des Advanced Proxy ausgenommen sind (Zeit, Größe, Browserprüfung, etc.) und welche IP- oder MAC-Adressen komplett gesperrt sind.

Wie gerade erwähnt gibt es Einschränkungen, die nachfolgend konfiguriert werden. Zum einen kann die Betriebszeit des Proxys festgelegt werden. Unterschieden wird in Zulassen und Verweigern. Wobei Verweigern gleichzusetzen ist mit einem gesperrten Webzugriff. Es können

auch Transfergrenzen angegeben werden. Somit können etwa große Downloads von Filmen, CD-Images oder großen Archiven unterbunden werden. Die Einstellung *0* schaltet die Begrenzung aus. Zusätzlich zur Transfergrenze kann auch eine Downloaddrosselung konfiguriert werden. Diese kann pro Netzwerk (grün oder blau) ganz allgemein und speziell pro Host angegeben werden. Auch kann die Downloaddrosselung nur für bestimmte Inhalte aktiviert werden, um etwa bei großen Downloads anderen Clients noch genügend Bandbreite zur Verfügung zu stellen.

Die Angabe von MIME-Types ist eine weitere Möglichkeit bestimmte Inhalte zu blockieren. Um etwa den Download von PDF-Dateien zu unterbinden, genügt die Angabe des MIME-Types *application/pdf* und die Aktivierung des MIME-Type-Filters.

Eine weitere Möglichkeit den Zugriff auf den Proxy und damit aufs Web zu Beschränkung ist die Prüfung des verwendeten Browsers. So können beispielsweise nur die Browser Internet Explorer und Firefox aktiviert werden. Das Browsen über andere UserAgents ist damit dann nicht mehr möglich.

Weiterhin können der UserAgent und der Referer manipuliert werden. Die Änderung des UserAgents und/oder des Referers kann vorgenommen werden, um etwa die Identität des Browsers und Herkunft der letzten URL zu verschleiern, Obwohl dies zu zweifelhaften Ergebnissen im Browser führen kann.

Falls weitere AddOns installiert sind die auf den Advanced Proxy basieren (Update-Accelerator und URLfilter) können diese ebenfalls aktiviert werden.

Die letzte Option zur Konfiguration ist die Einstellung der Authentifizierungsmethode. Je nach eingestellter Methode gibt es dazu einen jeweiligen Einstellungsdialog. Nachfolgend ist die Methode der Windowsauthentifizierung beschrieben, da diese in den meisten Unternehmen vorhanden ist. Prinzipiell gibt es globale Einstellungen für alle Methoden. Dazu gehört die Anzahl der Prozesse die für die Authentifizierung verantwortlich sind. Ebenso die Zeit in der die Authentifizierung ohne weiter Benutzeraktion gültig ist. Auch kann eingestellt werden, mit wie vielen IP-Adressen der Benutzer angemeldet ist um somit ein mehrfaches Anmelden an unterschiedlichen Clients zu verhindern. Ebenfalls wichtig ist die Möglichkeit, dass Domains angegeben werden können die ohne Authentifizierung besucht werden dürfen. Dazu gehören etwa die Windows- oder Antivirenupdateserver.

Um die Windowsauthentifizierung durchführen zu können, muss noch der Domänenname sowie der Name des ActiveDirectory Servers angegeben werden. Sofern die integrierte Windows-

Authentifizierung aktiviert ist, werden die Anmeldeinformationen des angemeldeten Benutzer verwendet. Dieser braucht somit keine Daten mehr zur Anmeldung eingeben. Ansonsten wird der Benutzer ausdrücklich nach Benutzername und Passwort gefragt.

Auch hier kann nochmal eine Zugriffsbschränkung auf Benutzerebene erfolgen. Dazu wird eine Positiv- und eine Negativ-Liste verwendet, die den Zugriff auf das Internet über den Benutzernamen regelt[41].

5.3.1 Update Accelerator

Der Update Accelerator arbeitet ähnlich wie ein Proxyserver. Er cached bereits heruntergeladene Dateien und liefert diese bei erneuter Anforderung direkt aus seinem Cache aus. Der Unterschied zwischen einem Proxy und dem Update Accelerator liegt jedoch in der Eigenschaft der Größe der gecachten Dateien. Ein Service Pack für Windows ist mitunter mehrere hundert Megabyte groß und würde von einem Proxyserver daher nicht mehr gecached werden können. Dieser unterliegt in der Regel einer Größenbeschränkung. Bei einem Proxyserver liegt diese in der Regel bei mehreren hundert Kilobytes pro Datei. Auch würde der zur Verfügung stehende Plattenplatz bei einer zu hohen Angabe der Dateigröße sehr schnell aufgebraucht sein. Dies beeinflusst den Proxyserver wiederum negativ. Die Funktion ist daher ebenfalls vergleichbar mit einem Fileserver der unabhängig vom Proxy seine Inhalte bereithält[45].

Der Update Accelerator speichert die Dateien bei der ersten Anforderung automatisch. Jeder weitere Download der Datei wird vom Update Accelerator aus dem Cache ausgeliefert. Es werden die Updates der Hersteller Adobe, Apple, Avast, Linux, Microsoft, Symantec und Trend Micro gespeichert. Es ist allerdings möglich weitere Quellen zu definieren[46].

Installation Das heruntergeladene Paket wird auf den IPCop in ein temporäres Verzeichnis kopiert und dort mit tar entpackt. Die Installation wird danach im durch tar erstellten Verzeichnis durch Eingabe des Befehls *./install* gestartet. Die Installation läuft vollautomatisch durch[45].

Konfiguration Da der Update Accelerator auf den Advanced Proxy basiert, muss dieser erst im Menüpunkt des Proxys aktiviert werden. Auch für diese Funktion kann ein separates Logging aktiviert werden. Dieses ist jedoch nicht im Logmenü zu finden, sondern es befindet sich unter */var/log/updatexlrator/cache.log* auf dem IPCop.

Der Update Accelerator unterscheidet zwischen einem aktiven und einem passiven Modus. Im passiven Modus werden keinen neuen Updates aus dem Internet in den Cache gespeichert. Der passive Modus wird zudem automatisch ausgewählt sobald die Einstellung für den maximal verwendeten Speicherplatz überschritten ist. Diese darf auch nicht zu hoch eingestellt werden, da ansonsten die Festplatte des IPCops zu schnell voll läuft.

Ebenfalls konfiguriert werden kann die Frequenz in der die Updates auf Aktualisierungen überprüft werden. Diese kann aktiviert oder deaktiviert werden und es kann eingestellt werden, ob die veralteten Dateien entfernt werden sollen. Wird diese Option deaktiviert, bleiben Sie im Cache bestehen, werden jedoch entsprechend markiert.

Sobald sich Dateien im Cache befinden, können diese auch verwaltet werden. Zum Einen lassen sich anhand der Statistik überprüfen wie viele Updates von welcher Quelle sich im Cache befinden und wie der Status dieser Quellen ist. In der Wartungsansicht lassen sich darüber hinaus die einzelnen Dateien herunterladen, oder aber auch gezielt löschen[40].

5.3.2 Calamaris

Das AddOn Calamaris [39] für den Advanced Proxy ist ein Tool, welches das Logfile des Proxys analysiert und auswertet um daraus einen Bericht zu erstellen. Es wurde von Cord Beermann entwickelt[3]. Mit Calamaris können sehr einfach und flexibel detaillierte Proxyberichte generiert werden. Der Bericht enthält eine Zusammenfassung, eine Aufschlüsselung nach der Methode der Abfrage (GET, POST, HEAD) und eingehendem und ausgehendem Verkehr, er unterscheidet nach Protokoll, Größe und Typ der Objekte und zeigt Infomationen über die Effizienz des Proxys[44].

Die Installation erfolgt nachdem das Paket auf den IPCop übertragen und dort mittels tar entpackt wurde. Die Installation kann nach dem Entpacken durch Eingabe des Befehls *./install* gestartet werden. Calamaris befindet sich nach der Installation im Menüpunkt *Logs*. Dort kann nach Eingabe des Zeitraums für den der Bericht erstellt werden soll und Angabe der gewünschten Optionen die Erstellung des Bericht gestartet werden. Je nach Umfang kann dies eine gewisse Zeit dauern. Daher kann zusätzlich angegeben werden, dass archivierte Logdateien übersprungen werden sowie der Prozess zur Erstellung im Hintergrund läuft.

Sobald der Bericht erstellt wurde kann dieser im Browser angezeigt, zur weiteren Verarbeitung exportiert oder aber auch gelöscht werden sofern dieser nicht mehr benötigt wird.

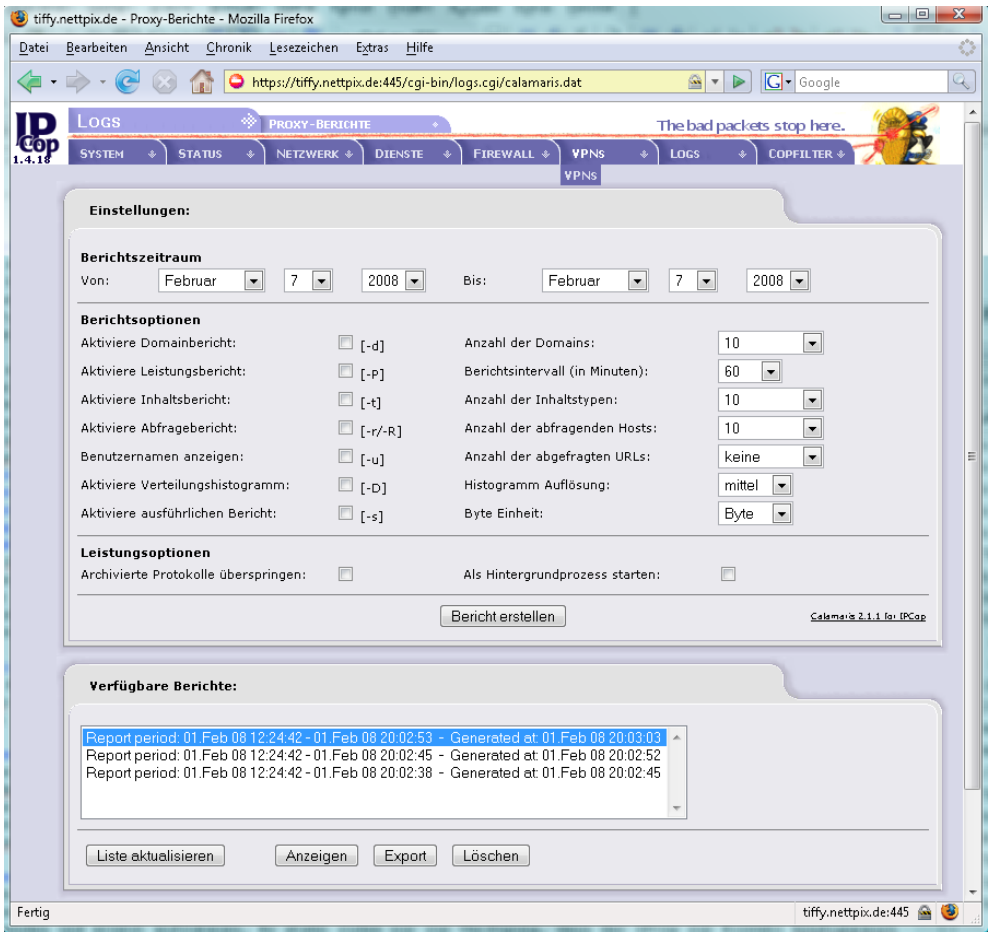

tiffy.nettpix.de - Proxy-Berichte - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://tiffy.nettpix.de:445/cgi-bin/logs.cgi/calamaris.dat
LOGS
PROXY-BERICHTE
The bad packets stop here.
SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS COPFILTER
VPNS
Einstellungen:
Berichtszeitraum
Von: Februar 7 2008 Bis: Februar 7 2008
Berichtsoptionen
Aktiviere Domainbericht: [-d] Anzahl der Domains: 10
Aktiviere Leistungsbericht: [-P] Berichtsintervall (in Minuten): 60
Aktiviere Inhaltsbericht: [-t] Anzahl der Inhaltstypen: 10
Aktiviere Abfragebericht: [-r/-R] Anzahl der abfragenden Hosts: 10
Benutzernamen anzeigen: [-u] Anzahl der abgefragten URLs: keine
Aktiviere Verteilungshistogramm: [-D] Histogramm Auflösung: mittel
Aktiviere ausführlichen Bericht: [-s] Byte Einheit: Byte
Leistungsoptionen
Archivierte Protokolle überspringen: Als Hintergrundprozess starten:
Bericht erstellen
Calamaris 2.1.1 for IPCop
Verfügbare Berichte:
Report period: 01.Feb 08 12:24:42 - 01.Feb 08 20:02:53 - Generated at: 01.Feb 08 20:03:03
Report period: 01.Feb 08 12:24:42 - 01.Feb 08 20:02:45 - Generated at: 01.Feb 08 20:02:52
Report period: 01.Feb 08 12:24:42 - 01.Feb 08 20:02:38 - Generated at: 01.Feb 08 20:02:45
Liste aktualisieren Anzeigen Export Löschen
Fertig
tiffy.nettpix.de:445

Abbildung 5.4: Screenshot Konfigurationsmaske Calamaris

Installation Das von der Projektseite heruntergeladene AddOn wird in ein temporäres Verzeichnis auf den IPCop übertragen. Dort wird es mittels tar entpackt und anschließend im entpackten Verzeichnis durch Eingabe des Befehls *./install* gestartet. Die Installation läuft automatisch durch und richtet einen zusätzlichen Menüpunkt im Logmenü ein[44].

Konfiguration Eine Konfiguration dieses AddOns ist nicht erforderlich. Jedoch stehen für die Erstellung eines Berichts einige Optionen zur Verfügung. Abbildung 5.4 zeigt die Maske zur Erstellung eines Berichts. Mit diesen Optionen lassen sich weitere detailliertere Informationen mit in den Bericht aufnehmen. Diese sind ein Domainbericht, der die am häufigsten aufgerufenen Domains enthält (Top- und 2nd-level). Ein Leistungsbericht, der Aufschluss über die Datenrate pro Stunde der Downloads gibt. Ein Inhaltsbericht, welcher die unterschiedlichen Inhalte (nach content-type und extension) wiederspiegelt, sowie ein Abfragebericht der alle Abfragen unterteilt nach UDP- und TCP-Abfragen enthält. Zusätzlich lässt sich ein Ver-

teilungshistogramm erstellen. Dieses zeigt die statistische Verteilung der Dateigrößen an. Zu allen Optionen lassen sich weitere Einstellungen bezüglich der Detailtiefe einstellen. Die Erstellung der Berichte kann abhängig von der Detailtiefe zwischen einer und drei Minuten dauern[44].

5.4 URL filter

Das URL filter AddOn wird dazu eingesetzt unerwünschte Seiten nach Kategorien sortiert wie etwa Pornografie, Gewalt oder Spiele im Netzwerk zu sperren. Die Sperrung erfolgt anhand einer dem SquidGuard kompatiblen Blacklist. Diese kann zudem in regelmäßigen Abständen automatisch aktualisiert werden. Ein weiteres Merkmal ist die Steuerung auf zeitlicher und clientbasierter Ebene. Voraussetzung für die Funktionalität des URL filter ist der Einsatz des Proxys. Dieser muss entweder auf den Clients eingetragen sein oder der Proxy muss im transparenten Modus arbeiten. Alternativ kann auch das Web Proxy Autoconfig Discovery AddOn des Advanced Proxy oder ein ProxyScript genutzt werden, um die Proxy IP-Adresse zu verteilen[49].

Installation Das AddOn wird, nachdem es heruntergeladen wurde, auf den IPCop in ein temporäres Verzeichnis kopiert. Danach wird das Paket mit tar entpackt und die Installation wird im daraufhin erstellten Verzeichnis durch Eingabe von *./install* gestartet. Die Installation läuft vollautomatisch ab[47].

Konfiguration Die Konfiguration des URL filter gliedert sich in zwei Bereiche, den URL filter Einstellungen und der Wartung. Im Bereich der Einstellungen werden zunächst die Sperrkategorien ausgewählt. In der derzeitigen Version stehen folgende Kategorien zur Auswahl:

- ads (Werbung)
- gambling (Glücksspiele)
- proxy
- aggressive
- hacking
- violence (Gewalt)
- audio-video
- mail

- warez (Illegale Softwarebeschaffung)
- drugs (Drogen)
- porn (Pornos u.ä.)

Zusätzlich kann eine eigene White- und Blacklist gepflegt werden, in der IP-Adressen und Full Qualified Domain Names (FQDN) eingetragen werden können (dazu auch Subdomains). Außerdem gibt es die Möglichkeit eigene (reguläre) Ausdrücke zu hinterlegen auf die der URL filter anspringen soll. Ebenso ist es möglich ganze Dateitypen zu sperren. Diese sind in drei Gruppen gegliedert.

- Ausführbar
- Archive
- Audio-/Videodateien

Zu der allgemeinen Filterung enthält der URL filter verschiedene Arten der Zugriffskontrolle. Diese kann zum einen netzwerkbasiert erfolgen, um zu entscheiden, ob ein Client generell gesperrt ist oder ob ein Client von der Filterung ausgenommen ist. Dazu wird entweder die IP-Adresse oder ein IP-Range eingetragen. Die zweite Möglichkeit der Zugriffskontrolle ist die Vergabe von Zeitkontingenten. Diese kann generell für den URL filter definiert werden, um etwa die Filterung während der normalen Geschäftszeiten zu aktivieren, aber auch um bestimmten Benutzern ein Zeitlimit pro Tag zu gewähren.

Ist der URL filter aktiv und auf eine geblockte Seite gestoßen wird dem Benutzer ein Warnung im seinem Browser angezeigt. Dazu können zusätzliche Informationen im Bereich der Sperrseiteneinstellung definiert werden. Es kann ausgewählt werden, ob die Sperrkategorie, die Adresse und die Client-IP-Adresse auf der Sperrseite angezeigt werden soll. Außerdem kann ein Hintergundbild eingestellt werden, etwa um das Corporate Design eines Unternehmens zu wahren. Alternativ kann auch auf eine eigene Seite umgeleitet werden. Um dem Benutzer mitzuteilen was genau vorgefallen ist, existieren noch drei zusätzliche Felder, in denen Text hinterlegt werden kann. Diese werden ebenfalls auf der Sperrseite angezeigt.

Als letztes können noch erweiterte Einstellungen konfiguriert werden. Etwa, ob ein Log aktiviert ist und in Kategorien aufgeteilt werden soll, wie viele Filterprozesse aktiv sind (entscheidend für die Geschwindigkeit je nach der eingesetzten Hardware) oder ob beispielsweise generell alle URLs oder nur URLs mit IP-Adressen gesperrt sind.

Durch Anklicken des Schalters Speichern und Neustart wird der URL filter aktiviert.

Die Wartung gestaltet sich etwas einfacher als die Konfiguration. Zum einen kann eine eigene Blacklist auf den IPCop hoch geladen werden. Diese wird in die Datenbank des URL filter mit aufgenommen. Die hochzuladende Datei muss im Format tar.gz sein. Es kann allerdings auch ein externer Dienstleister in Anspruch genommen werden wodurch der URL filter automatisch aktualisiert wird. Dazu stehen drei Dienstleister zur Verfügung, zwei auf internationaler Ebene sowie einer aus Deutschland.

- Shalla Secure Service (deutscher Service)
- Multnomah Education Service District (MESD)
- Univerity Toulouse

Um eigene Blacklisten zu erstellen bietet der URL filter einen eigenen Blacklist-Editor. Innerhalb dieses Editors können die zu sperrenden URLs und Domains den verschiedenen Kategorien zugeordnet werden. Ebenso können weitere Kategorien erstellt werden. Die erstellte Blacklist kann nach der Erstellung zur Übertragung auf andere Systeme exportiert werden wie auch eine fremde Liste importiert werden kann.

Jede Änderung an der Datenbank des URL filter erfordert dessen Neustart[48].

5.5 Copfilter

Dieses AddOn umfasst ein ganzes Paket nützlicher und sinnvoller Zusatzfunktionen. Es umfasst im wesentlichen einen Proxyserver, auf Basis des Proxys Privoxy, zum Schutz der Dienste POP3, SMTP, HTTP und FTP vor Viren sowie einen umfassenden E-Mail Schutz. Der Virenscan wird zum einen von dem mitgeliefertem Scanner ClamAV übernommen. Zum anderen kann der Virenscan durch zusätzliche Installation der Anti-Virenprogramme F-Prot und AVG erweitert werden. Diese sind für den kommerziellen Gebrauch kostenpflichtig und müssen per anno lizensiert werden. Nachteilig ist, dass die erforderliche Hardwareanforderung sprunghaft steigt und mit wachsender Zahl der Clients weiter zunimmt. Ein wesentlicher Faktor hierbei sind zum einen die CPU, die für die Erkennung von SPAM erforderlich ist sowie die Größe des Arbeitsspeichers, da dieser zum Großteil vom Virenscanner genutzt wird. Ein weiterer Faktor liegt in der Zeit, die für die Prüfung auf Viren gewartet werden muss. Beim Surfen machen sich daher zum Teil Latenzen bemerkbar[31].

Der Entwickler dieses AddOns betreibt eine eigene Website, `http://www.copfilter.de` und eine eigenes Forum, `http://copfilter.endlich-mail.de`. Dem Benutzer

tiffy.nettpix.de - Copfilter - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://tiffy.nettpix.de:445/cgi-bin/copfilter_status.cgi
COPFILTER STATUS
The bad packets stop here.
SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS COPFILTER
Copfilter
Version: 0.84beta3a
Dokumentation: README CHANGELOG CREDITS BUGS
WARNUNG: Dieses Paket ist KEIN offizielles IPCop-Addon. Es wurde weder durch die IPCop-Entwickler programmiert noch besichtigt. Es gibt keine Garantie, die Benutzung erfolgt auf eigene Gefahr. Dieses Paket fügt Firewall-Regeln, Proxies, Filter und Viren-Scanner auf dem IPCop hinzu. Benutze NICHT den Copfilter, wenn Dir die Sicherheit des IPCop wichtig ist. Trotz Einsatz von HAVP könnte es möglich sein, dass ein Virus empfangen wird.
Virus Quarantine (10x)
Spam Quarantine (13x)
Monit Service Manager
Copfilter Whitelist Manager
Copfilter Spam Übersichts-Manager
Produkt Beschreibung Dienst Version Status Manuelle Kontrolle*
monit Überwachungsdienst monit 4.9 ON (PID 31716 14220 14219) Stoppe monit
P3Scan Transp. POP3 Proxy p3scan 2.2.1 ON (PID 11970) Stoppe p3scan
ProxSMTP Transp. SMTP Proxy proxsmtpd 1.6 ON (PID 14509 13518) Stoppe proxsmtpd
HAVP Transp. HTTP Proxy havp 0.86 ON (PID 14487 14486 ...) Stoppe havp
Privoxy Transp. HTTP Proxy privoxy 3.0.6 ON (PID 14138 14136) Stoppe privoxy
frox Transp. FTP Proxy frox 0.7.18 OFF Starte frox
SpamAssassin AntiSpam Filter spamd 3.2.3 ON (PID 31828 31827 31811) Stoppe spamd
ClamAV AntiVirus Programm clamd 0.91.2/5728 ON (PID 12786 12584) Stoppe clamd
AVG** AntiVirus Program avgscan 7.5.51 OFF Start avgscan
F-PROT*** AntiVirus Programm no daemon 4.6.8 ON ACCESS (no pid)
Renattach Attachment Renamer no daemon 1.2.4 OFF
Rules Du Jour AntiSpam Regelsätze no daemon 1.30 ON ACCESS (no pid)
starte alle Dienste neu
.. alle Einstellungen werden übernommen
AntiVirus Statistik - text (ClamAV, sofortiges Update)
AntiVirus Statistik - grafisch (ClamAV, wöchentliche Updates, beginnt nach der 1. Woche)
AntiSpam Statistik - text (SpamAssassin)
HTTP Virus Log - text (HAVP)
Fertig
tiffy.nettpix.de:445

Abbildung 5.5: Screenshot Startseite des Copfilter AddOns

des AddOns steht somit neben der Community für den IPCop eine zwei weitere Quellen zum direkten Anlauf bei Problemen zur Verfügung, .

Installation Das AddOn wird von der Projektseite heruntergeladen und in einem temporärem Verzeichnis mittels tar entpackt. Die Installation wird im nun erstellten Verzeichnis durch Eingabe von *./install* gestartet und erwartet die Bestätigung vom Benutzer, dass die Installation fortgeführt werden darf. Danach läuft sie automatisiert durch[32, Seite 10].

Konfiguration Nach der Installation befindet sich im WebGUI des IPCop der zusätzliche Hauptmenüpunkt *Copfilter*. Der Untermenüpunkt *Status* gibt zunächst einen Überblick über die laufenden Dienste des Copfilters. Nach der Installation sind diese alle deaktiviert.

Auf der Statusseite siehe Abbildung 5.5 befinden sich zudem weitere Funktionen. So sind hier die Quarantäne Seiten der Viren- und SPAM-Funde zu erreichen wie auch die Whitelist für den SPAM-Filter. Ebenso sind zu diesen Diensten zahlreiche Statistiken abrufbar.

Damit der Copfilter ordnungsgemäß läuft, ist es erforderlich, im Punkt E-Mail die Einstellungen für ein E-Mail-Postfach zu hinterlegen. Dazu wird eine E-Mail-Adresse als Empfänger und eine als Absender hinterlegt. Ebenso müssen ein SMTP-Server sowie die Daten zur SMTP-Authentifizierung hinterlegt werden. Es ist durchaus sinnvoll, für den IPCop ein eigenes Postfach einzurichten, da der Monit-Dienst des Copfilters regelmässig Reports an diese Adresse sendet. Somit sind alle wichtigen E-Mails über den Status der Firewall und der laufenden Dienste an zentraler Stelle abgelegt[32, Seite 19].

Die Konfiguration der weiteren Dienste ist nachfolgend detailliert beschrieben.

5.5.1 Quarantäne

Es sind zwei Quarantänebereiche vorhanden. Einer beinhaltet die gefundenen E-Mails, die einen Virus enthalten, der andere, wie es Abbildung 5.6 darstellt, enthält alle unter SPAM-Verdacht identifizierten E-Mails. Der Aufbau ist in beiden Bereichen identisch. Es sind Absenderadresse, Empfängeradresse und Betreff tabellarisch aufgelistet. Dazu kommt eine Zeitstempel und ein Dateiname unter dem die E-Mail in der Quarantäne abgelegt ist. Im Bereich der Virusquarantäne existiert zudem eine Spalte, welche den gefunden Virus namentlich kennzeichnet. In beiden Bereichen ist es möglich durch Markieren einer Checkbox eine Auswahl bestimmter E-Mails dem eigentlichen Empfänger zukommen zu lassen, etwa bei False-Positive Funden. Des Weiteren kann die Quarantäne gänzlich geleert werden[32, Seite 40].

5.5.2 Monit

Monit ist die zentrale Steuerung des Copfilters. Monit ist ein Dienst, der die weiteren Dienste des Copfilter überwacht und bei Änderung des Zustands eines Dienstes eine E-Mail an den Empfänger sendet und ihn so darüber in Kenntnis setzt. Der Dienst wird im Untermenüpunkt *Überwachung* durch Setzten der Combobox auf *On* und Anklicken des Schalters *speichern* gestartet. Über den neben der Combobox stehenden Link gelangt der Benutzer zum Monit Server Manager. Dies ist eine eigene per Secure Socket Layer (SSL) verschlüsselte Website

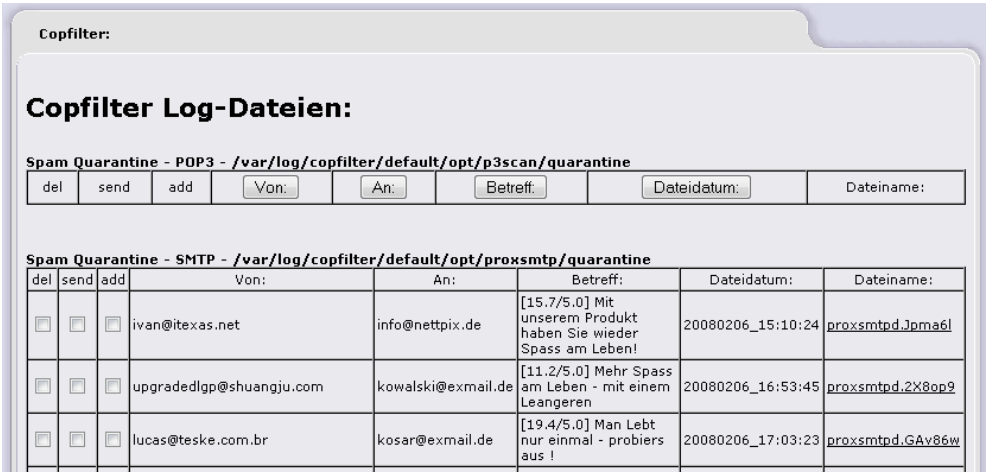

Copfilter:
Copfilter Log-Dateien:
Spam Quarantine - POP3 - /var/log/copfilter/default/opt/p3scan/quarantine
del send add Von: An: Betreff: Dateidatum: Dateiname:
Spam Quarantine - SMTP - /var/log/copfilter/default/opt/proxsmtp/quarantine
del send add Von: An: Betreff: Dateidatum: Dateiname:
ivan@itexas.net info@nettpix.de [15.7/5.0] Mit unserem Produkt haben Sie wieder Spass am Leben! 20080206_15:10:24 proxsmtpd.Jpma6l
upgradedlgp@shuangju.com kowalski@exmail.de [11.2/5.0] Mehr Spass am Leben - mit einem Leangeren 20080206_16:53:45 proxsmtpd.2X8op9
lucas@teske.com.br kosar@exmail.de [19.4/5.0] Man Lebt nur einmal - probiers aus ! 20080206_17:03:23 proxsmtpd.GAv86w

Abbildung 5.6: Screenshot Quarantäne des Copfilters

für den Dienst Monit, welche auf der Firewall auf dem Port 446 läuft. Die Zugangsdaten entsprechen denen des IPCops.

Nach erfolgter Authentifizierung erhält der Benutzer weiterführende Informationen zu den laufenden Diensten des Copfilters. Dies sind neben dem Status unter anderem CPU-Last, Uptime und Speicherverbrauch. Detailliertere Informationen erhält der Benutzer durch Anklicken des Links für den jeweiligen Dienst. Alle Dienste können hier gestoppt, gestartet oder auch deaktiviert werden.

Da Monit alle Dienste überwacht, sendet er bei jeder Statusänderung an das hinterlegte E-Mail-Postfach einen Report. Dieser enthält Informationen über die jeweilige Änderung[32, Seite 20].

5.5.3 P3Scan

P3Scan ist ein Dienst, der den einkommenden E-Mail-Verkehr im POP3 Protokoll untersucht. Der Dienst kann für die Netzwerke grün, orange und blau separat eingeschaltet werden. Bei der Untersuchung einer E-Mail kann auch entschieden werden, ob ein Kommentar dazu in der E-Mail hinterlegt werden soll. Dies kann im E-Mail-Header als auch im Body-Text erfolgen. Zudem kann eingestellt werden, ob der Betreff einer erkannten SPAM-E-Mail verändert werden. Dem Betreff wird dann der Text „*** SPAM ***“ vorangestellt. Dies erleichtert das nachträgliche manuelle oder regelbasierte Ausfiltern im E-Mail-Client, da das POP3 Protokoll keine Unterdrückung der E-Mail erlaubt. Dennoch ist es möglich erkannte SPAM-Emails in

den Quarantäne Ordner zu verschieben. Um nicht jede E-Mail prüfen zu müssen existiert eine White- und eine Blacklist. Jeder ausgehende E-Mail-Empfänger kann in dieser Liste automatisch eingetragen werden. Daneben besteht jedoch auch die Möglichkeit die Liste manuell zu bearbeiten.

Neben der SPAM-Erkennung ist auch eine Prüfung der E-Mail auf Viren oder verdächtige Anhänge vorhanden. Diese Funktionen können wiederum separat zugeschaltet werden. Da, wie bereits erwähnt, ein Unterdrücken der Nachricht nicht möglich ist, wird die E-Mail soweit modifiziert, dass der Empfänger nur einen Hinweis erhält, dass die E-Mail einen Virus enthielt. Ebenso wie bei der SPAM-Erkennung kann auch die Virenerkennung die Originalnachricht in die Quarantäne verschieben. Die Quarantäne kann zudem automatisiert nach einer Voreinstellung turnusmäßig nach Ablauf einer Zeitspanne geleert werden[32, Seite 22].

5.5.4 ProxSMTP

Die meisten Einstellungen für den ProxSMTP-Dienst korrespondieren im wesentlichen mit denen des P3Scans. Zusätzlich können jedoch weitere Funktionen eingestellt werden. Zuerst können Einstellungen für den ausgehenden SMTP-Verkehr eingestellt werden. Dies kann, wie bei P3Scan, für die unterschiedlichen Netzwerke definiert werden. Ebenso kann wieder ein Kommentar eingefügt werden wie auch eine Veränderung des Betreffs möglich ist. Genauso kann auch die Virenerkennung eingeschaltet werden.

Neben dem ausgehenden Scan ist auch ein Scan der eingehenden E-Mails möglich. Dazu muss der Dienst auf der roten Schnittstelle aktiviert werden. Ebenso wird angegeben in welchem Netzwerk sich der eigene E-Mailserver befindet und unter welcher IP-Adresse und unter welchem Port dieser erreichbar ist. ProxSMTP macht somit ein Relaying zum eigenen E-Mailserver wodurch dieser zum OpenRelay-Server wird. Es ist daher zwingend erforderlich die eigene E-Mail-Infrastruktur auf ein OPenRelay hin zu prüfen. Dies kann beispielsweise unter `http://www.spamhelp.org/shopenrelay` oder bei `http://www.abuse.net/relay.html` erfolgen.

Wie beim P3Scan gibt es auch hier die Einbeziehung der White- und Blacklist. Auch die Quarantäne kann hier wierderum eingeschaltet werden. Diese hat jedoch hier eine wesentlich gewichtigere Bedeutung, da ProxSMTP die Aussonderung erkannter E-Mails vornimmt und diese dem Empfänger vorenthält. Die Quarantäne wird somit zur Versicherung, falls doch mal eine E-Mail irrtümlich als SPAM erkannt wird oder unter Virenverdacht fällt.

Da die E-Mails verworfen werden können, existiert noch eine weitere Einstellung zur Behandlung abgewiesener E-Mails. Diese können entweder unter Verwendung des SMTP Fehlercodes 550 abgelehnt werden oder unter Verwendung des Fehlercodes 250 verworfen werden. Dies hat aus Gründen des Datenschutz rechtliche Auswirkungen, da es einen Unterschied macht, ob eine Nachricht auf dem Weg vom Absender zum Empfänger abgewiesen wird, oder ob die Nachricht nach erfolgter Ablieferung beim E-Mailserver entfernt wird. Letzteres stellt einen Eingriff ins Postgeheimnis dar. Daher ist ebenso ratsam vor Installation eines solchen Dienstes in einem Unternehmen eine entsprechende Prüfung der Dienstanweisungen vorzunehmen, die eine Regelung zur Nutzung der IT-Infrastruktur beinhaltet[32, Seite 26].

5.5.5 HAVP

HAVP ist ein Proxydienst, der den eingehenden Datenverkehr in Verwendung von HTTP untersucht. HAVP erkennt unter mithilfe der Virenscanner Browser-Exploits, Viren oder Phishing-Versuche. Zudem ist es möglich, den HTTP-Datenstrom nach Werbe-Fenstern, Bannern oder Pop-Ups zu filtern, da HAVP dem Proxydienst Privoxy unterliegt. Um die sich im Netzwerk befindlichen Clients nicht manuell konfigurieren zu müssen, steht hier ebenfalls die Nutzung des Proxys im transparenten Modus zur Verfügung[32, Seite 30].

5.5.6 Privoxy

Privoxy selbst hat ähnlich wie Monit eine eigene Administrationsoberfläche. Diese ist unter der Adresse `http://config.privoxy.org` erreichbar. Diese Adresse wird intern in der Firewall umgeleitet und befindet sich nicht wie es aussieht im Internet, sondern in der Firewall selbst. Da Privoxy ein eigenständiges und mächtiges Produkt ist, wird an dieser Stelle zur Konfiguration auf die umfangreiche Dokumentation im Internet verwiesen `http://www.privoxy.org`. Provoxy wird als transparenter Proxy eingesetzt, da es damit erst möglich wird, die Inhalte aus POP3, SMTP und HTTP/FTP zu scannen.

5.5.7 frox

frox ist ähnlich wie HAVP ein Dienst, der den Datenverkehr überwacht. Frox überwacht jedoch den FTP Datenstrom. Privoxy ist wiederum Grundlage für den Dienst und wird ebenfalls

durch die installierten Virenscanner unterstützt. Die Nutzung des Dienstes kann auch hier für jedes Netzwerk separat aktiviert werden.

5.5.8 SpamAssassin

Die SPAM-Filter-Komponente im Copfilter übernimmt der Dienst SpamAssassin. Es ist eine freie Software, welche mittlerweile seit 2004 dem Projekt der Apache Software Foundation unterliegt. SpamAssassin ist ein intelligenter E-Mail-Filter, der anhand eine Regelwerks und verschiedener Mechanismen zwischen erwünschter und unerwünschter E-Mail zu unterscheiden versucht. Durch die modulare Architektur dieses Filters ist eine Integration in die unterschiedlichsten E-Mail-Systeme problemlos möglich. Dies ist neben den guten Erfolgsquoten bei der Erkennung von SPAM ein Grund für die Integration von SpamAssassin in den Copfilter[32, Seite 35][33].

Die Erkennung von SPAM unterliegt der kombinierten Bewertung durchgeführter Tests. Folgende Tests werden von SpamAssassin durchgeführt:

- Header Tests
- Ausdruckstest des Body textes
- Bayesfilter
- Automatische whitelist/blacklist Pflege
- Manuelle whitelist/blacklist Pflege
- Gemeinschaftliche SPAM Identifikationsdatenbank (DCC, Pyzor, Razor2)
- DNS Blocklisten (RBL)
- Zeichensatz und Sprachabhängigkeiten

Jeder Test für sich ergibt einen Wert. Anhand dieses Wertes lässt sich allerdings noch keine pauschale Aussage über die SPAM-Wahrscheinlichkeit treffen. Die Summe der Ergebnisse der einzelnen Test ergibt jedoch eine recht eindeutige Beurteilung der überprüften Nachricht. So kann eine unerwünschte Nachricht, die von einem Test fälschlicherweise als erwünscht eingestuft wurde dennoch ausgefiltert werden, sofern andere Tests eine eindeutige Identifizierung als SPAM ergeben. Die Zahl der false negatives sinkt. Zusätzlich lässt sich die Zahl der false positives verbessern, indem die Whitelist gepflegt wird.

Eine weitere Möglichkeit die Erkennungsrate zu verfeinern besteht darin den Bayesfilter zu trainieren. Dazu ist es erforderlich, dass in einem Postfach auf der obersten Ebene zwei Ordner mit den Namen *spam* und *not-spam* existieren. Zudem muss es möglich sein, dass dieses

Postfach über IMAP erreichbar ist. Das Training lässt sich manuell starten oder aber auch automatisiert einrichten, so dass das Training durch SpamAssassin in der Nacht erfolgt. Dies entlastet die Firewall, da das Training stark prozessorlastig ist und laut Dokumentation für 400 E-Mails rund. 1 Stunde dauert. Um erste Erfolge zu erhalten ist ein Minimum von 200 E-Mails in beiden Ordner notwendig.

SpamAssassin lässt sich über den Punkt *Copfilter* > *AntiSpam* konfigurieren. Zunächst lässt sich SpamAssassin ein- bzw. ausschalten und es kann der Wert angegeben werden, ab dem eine E-Mail im Betreff als SPAM markiert wird. Zusätzlich kann ein weiterer Dienst (Überprüfung der SPAM Identifikationsdatenbank Razor, DCC und DNSBL) zur SPAM Erkennung separat aktiveren. Dies ist besonders interessant bei der Nutzung des POP3 Filters, da hier die Überprüfung wie es aus den Logdateien ersichtlich ist, pro E-Mail ca. 30 Sekunden dauert. Einsicht in die Logdatei erhält der Benutzer ebenfalls über den Konfigurationsbildschirm des SpamAssassin. Hier kann eine Gesamtstatistik abgerufen werden, sowie eine detailliertere monatliche oder für den einzelnen Tag aufbereitete Statistik.

Weiterhin lässt sich die Erkennung des Bayesfilter manipulieren. Dazu können Feineinstellungen für das Ergebnis des Tests vorgenommen werden. So kann nach prozentualer Wahrscheinlichkeit ausgewählt werden, welchen Wert der Bayesfilter SpamAssassin mitteilt. Etwa eine Reduzierung des Gesamtwertes durch einen negativen Wert oder eine Erhöhung des Gesamtwertes durch einen positiven Wert. Die bereits voreingestellten Werte sind jedoch bereits so gut, dass hier vorerst keine Einstellung vorgenommen werden sollte. Nur bei zu hohen false positive und false negative Werten kann an diesen Werten eine Änderung vorgenommen werden, um die Erkennung zu verbessern.

Die letzten Einstellungen auf dieser Seite betreffen die Hinterlegung der Daten für das Postfach welches die *spam* und *not-spam* Ordner enthält, die Aktivierung der *SARE Rules* (SpamAssassin Rules Emporium) von Openprotect.com sowie ob und in welchem Zeitraum die Aktualisierung der Regeln vorgenommen werden soll.

5.5.9 Virenscanner

Copfilter unterstützt neben der SPAM-Erkennung in E-Mails auch die Überprüfung auf Viren. Dazu gehört zum Lieferumfang der frei erhältliche Virenscanner ClamAV. Aber auch die Integration zweier weiterer Virenscanner, nämlich F-Prot und AVG ist möglich. Für alle drei

Scanner gibt es einen gemeinsamen Konfigurationsbildschirm. In diesem lassen sich alle separat aktivieren. Zudem kann eingestellt werden, ob und in welchem Zeitraum der jeweilige Scanner automatisiert seine Updates erhält[32, Seite 41].

5.5.10 ClamAV

Da ClamAV zum Lieferumfang gehört, braucht es nicht separat installiert werden. ClamAV lässt im Gegensatz zu den anderen Scannern die Einstellung zu, ob verschlüsselte Archive generell als Viren betrachtet werden sollen. Diese Option kann deaktiviert bleiben, zumal es in jedem Unternehmen zum Standard gehört, dass ein Virenscanner am Arbeitsplatz eingerichtet ist. Dieser sollte spätestens beim Öffnen des verschlüsselten Archivs Alarm schlagen. Eine weitere Möglichkeit, die der Copfilter im Zusammenhang mit ClamAV bietet, ist die Einbindung der inoffiziellen Phishing Signaturen der Seite `http://www.sanesecurity.com/clamav`. Die Einbindung dieser Signaturen bleibt dem Administrator überlassen und hängt von seinem Vertrauen zur Quelle ab. ClamAV stellt zudem eine Statistik über die gefundenen Viren bereit.

5.5.11 F-Prot und AVG

Die Installation von F-Prot und AVG gestaltet sich ähnlich einfach wie die Installation des Copfilter Addons selbst. Das jeweilige Paket muss zunächst von der offiziellen Webseite heruntergeladen werden:

F-Prot: http://www.fprot.org/pub/fp-linux-ws.tar.gz

AVG: http://free.grisoft.com/softw/70free/setup/avg75flr-r45-a0973.i386.rpm

Danach werden die Pakete auf den IPCop kopiert. F-Prot wird mit tar nach root entpackt, das AVG Paket wird nach */var/log/copfilter/default* verschoben. Die Installation wird dann durch Starten der Copfilter Installation sowie der Angabe eines Parameters und des jeweiligen Pfads der Installationsdateien des Scanners durchgeführt[32, Seite 45].

F-Prot: /setup_util -f /root/fp-linux-ws.tar.tar[32, Seite 45]

AVG: /setup_util -avg avg75flr-r45-a0973.i386.rpm

Die Installation läuft automatisch durch. Weitere Einstellungen sind nicht notwendig.

5.5.12 Tests und Logs

Copfilter stellt zur Überprüfung des Copfilters auf seine Funktionen diverse Tests bereit. Zum Einsatz kommt hierbei die Testdatei EICAR (European Expert Group for IT-Security) `http://www.eicar.org/anti_virus_test_file.htm`. Es ist ein 68/70 Byte langer Zeichencode, der eingefügt in eine Textdatei ein ausführbares Programm darstellt und die Meldung EICAR-STANDARD-ANTIVIRUS-TEST-FILE! ausgibt. Das Programm ist harmlos, muss aber von jedem Virenscanner als Virus erkannt werden. So lassen sich beispielsweise auch Archive mit einem Virenscanner prüfen, wenn diese Datei sich in einem solchen Archiv befindet. Eine ähnliche Datei gibt es für den SPAM Test, genannt GTUBE (Generic Test for Unsolicited Bulk Email). SpamAssassin wird eine E-Mail mit diesem String zu 100% als SPAM erkennen und ablehnen. Im Menüpunkt *Test & Logs* stehen drei Funktionen dazu bereit[32, Seite 44]:

- Virus E-Mail
- Spam E-Mail
- E-Mail mit gefährlichem Anhang

Zusätzlich zu diesen drei Tests befinden sich auf dieser Seite zwei Links zu Seiten auf denen die EICAR-Testdatei heruntergeladen werden kann. Einmal auf dem Weg über HTTP und einmal über FTP. In beiden Fällen sollte entweder HAVP oder frox, sofern aktiviert, den Download verweigern.

Auswertungen zu den einzelnen Funktionen des Copfilters stehen dem Benutzer ebenfalls auf dieser Seite zur Verfügung. Alle Logs enthalten detaillierte Informationen zu Status, Update, Fund, Fehlermeldungen und Verlauf der jweiligen Funktion.

5.6 High Availability - Ucarp

In Unternehmen in denen eine ständige Verfügbarkeit des Internet lebensnotwendig ist wird eine hohe Verfügbarkeit der eingesetzten Hard- und Software verlangt. Dazu wurde das High Availability AddOn auch Ucarp genannt von Markus Hoffmann entwickelt. Es hat die Aufgabe, einen zweiten IPCop, der als HotStandby neben dem primären System läuft, (im Notfall) dazu zuschalten falls der erste defekt ist. Für diese Anwendung sind mindestens zwei IPCop's und zwei Switche nötig. Die Einstellungen für die rote Schnittstelle müssen identisch sein. Für die grüne Schnittstelle werden zwei IP-Adressen aus demselben Subnetz benötigt.

Danach kann das AddOn auf beiden Maschinen installiert werden. Abbildung 5.7 zeigt eine schematische Anordnung bei zusätzlicher Nutzung einer DMZ. Die Farben der Verbindungen entsprechen denen der jeweiligen Schnittstelle. Alle Netzwerkbereiche sind weiterhin voneinander getrennt[25].

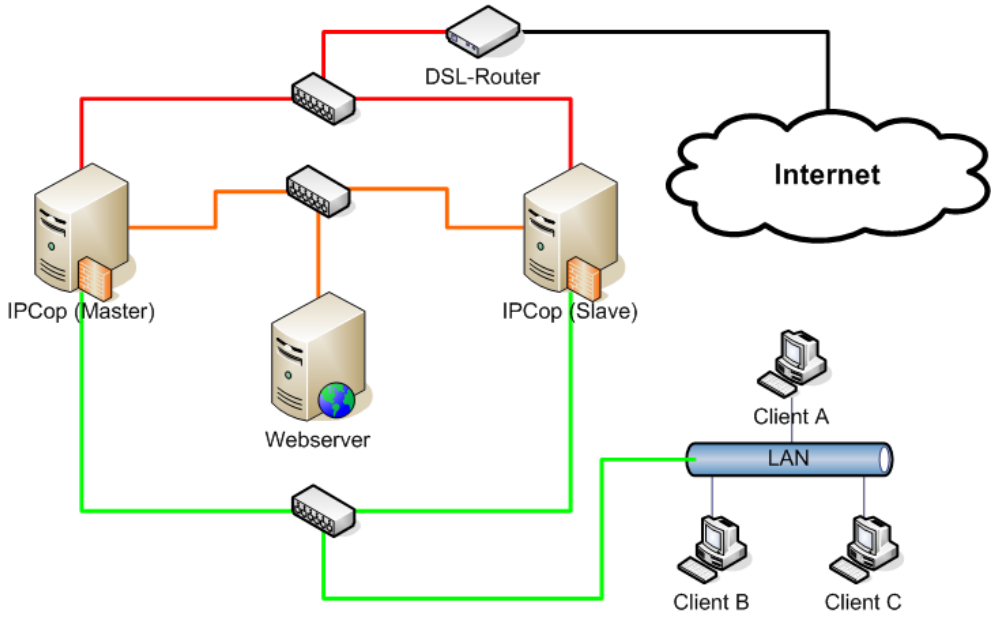


Abbildung 5.7: Schema des High Availability AddOns - Ucarp[25]

Installation Das AddOn wird auf den IPCop in ein temporärers Verzeichnis kopiert und mit tar entpackt. Das Installationsskript wird danch im erstellten Verzeichnis durch Eingabe des Befehls *./install* gestartet. Während der Installation erfolgt die Nachfrage, ob ein Versionscheck des AddOns gewünscht ist. Dies kann der Benutzer nach Belieben beantworten[22].

Konfiguration Die Konfiguration beginnt bei dem IPCop, der den HotStandby übernimmt. Dazu wird zunächst eine virtual ID vegeben. Diese ist eine interne ID für das Addon und muss auf beiden IPCop's identisch sein. Danach erfolgt die Eingabe der virtuellen IP-Adresse, die als Standardgateway fungiert. Diese wird nach erfolgter Installation in den Clients eingetragen. So ist sichergestellt, dass immer einer der beiden Cops je nach Zustand erreichbar ist. Wird ein Proxyserver verwendet, ist dies ebenfalls die IP-Adresse dafür. Die nun folgende Advertisement frequency ist der Zeitraum, den der Backup-IPCop wartet bevor er den Master-IPCop auf Funktion prüft. Der Wert ist in Sekunden angegeben. Die advertisement skew legt

den bevorzugten Master fest. Der Master erhält einen niedrigeren Wert als der Backup IPCop. Somit ist es möglich, ein beliebige Anzahl an IPCops zu verwenden. Wird die Verbindung nun überprüft, kann es vorkommen, dass die Anfrage nicht beantwortet wird, obwohl die Verbindung (der Master) in Ordnung ist. Dazu wird die deadratio festgelegt. Sie gibt an nach wie vielen negativen Antworten der Backup zum Master wird. Als nächstes wird ein Passwort vergeben mit dem sich die IPCops untereinander authentifizieren. Zum Schluss wird die reale grüne IP-Adresse des jeweils anderen IPCops eingetragen. Es folgt nun die Konfiguration des Masters. Diese ist identisch mit der des IPCops für den HotStandby.

Weiterhin einzustellen sind die Optionen für den Onlinecheck. Dazu können diverse Hosts angegeben werden, die in regelmässigen Abständen überprüft werden. Die Abstände können ebenfalls frei definiert werden. Ebenso kann die Zeit eingestellt werden nach der die beiden IPCops synchronisiert werden[25].

5.7 Webalizer

Das Webalizer AddOn wurde von Patrick Frei geschrieben und von S. Feddersen um ein Installationsskript erweitert. Es ermöglicht eine grafisch aufbereitete Einsicht in die Statistik über die Verwendung des Proxys[20].

Installation Die Installation erfolgt durch Kopieren des Pakets in ein temporäres Verzeichnis auf den IPCop und anschließendes Entpacken mit tar. Danach erfolgt die Ausführung des Befehls *./install* im durch tar erstellten Verzeichnis. Das Installationsskript erwartet beim Start die Eingabe der Option *i* um die Installation durchzuführen. Die Eingabe von *e* beendet die Installation vorzeitig[17].

Konfiguration Das AddOn nimmt seinen Platz im Menü *Status* ein. Es muss dort über die Checkbox *Webalizer aktivieren* gestartet werden. Zudem kann ein Zeitintervall angegeben werden in welchem Abstand die Erstellung der Statistiken vorgenommen wird. Eine Übersicht über den Zeitraum von 12 Monaten zeigt Abbildung 5.8[17].

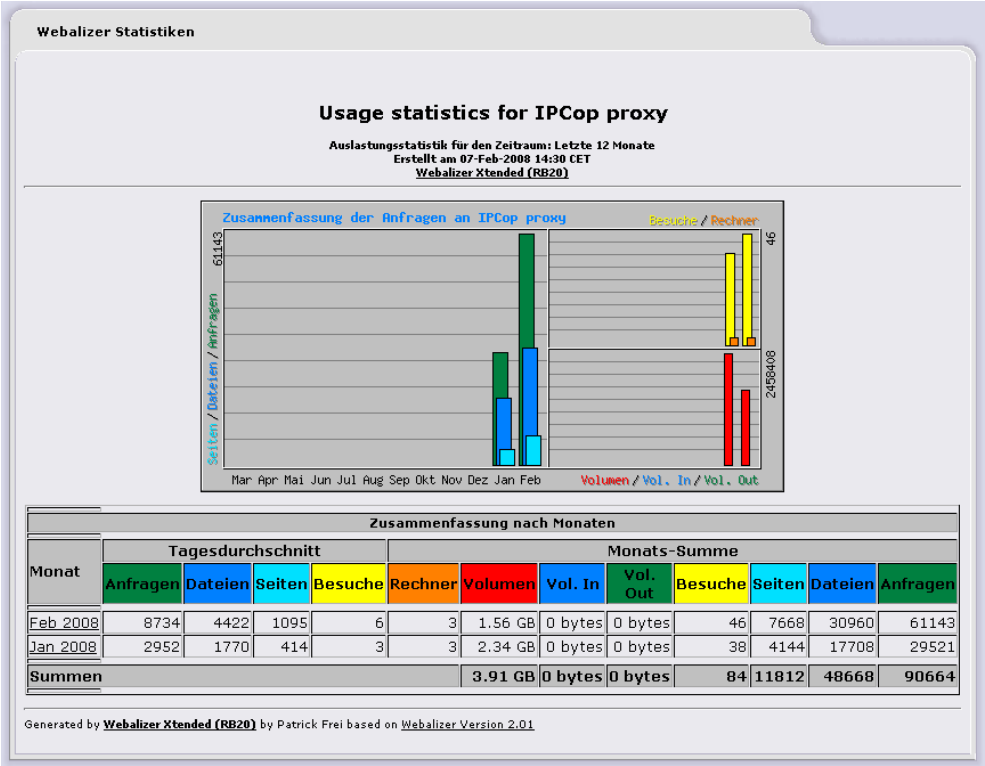

Webalizer Statistiken
Usage statistics for IPCop proxy
Auslastungsstatistik für den Zeitraum: Letzte 12 Monate
Erstellt am 07-Feb-2008 14:30 CET
Webalizer Xtended (RB20)
Zusammenfassung der Anfragen an IPCop proxy
Besuche / Rechner
Seiten / Dateien / Anfragen
61143
46
2458408
Mar Apr Mai Jun Jul Aug Sep Okt Nov Dez Jan Feb
Volumen / Vol. In / Vol. Out
Zusammenfassung nach Monaten
Monat
Tagesdurchschnitt
Monats-Summe
Anfragen Dateien Seiten Besuche Rechner Volumen Vol. In Vol. Out Besuche Seiten Dateien Anfragen
Feb 2008 8734 4422 1095 6 3 1.56 GB 0 bytes 0 bytes 46 7668 30960 61143
Jan 2008 2952 1770 414 3 3 2.34 GB 0 bytes 0 bytes 38 4144 17708 29521
Summen 3.91 GB 0 bytes 0 bytes 84 11812 48668 90664
Generated by Webalizer Xtended (RB20) by Patrick Frei based on Webalizer Version 2.01

Abbildung 5.8: Screenshot Bericht des Webalizer AddOns

5.8 LineTest

Mit dem AddOn Linetest ist es möglich eine Internetverbindung zu überwachen, um dann bei Problemen der Verbindung zu einer anderen Verbindung zu wechseln. Dazu wird eine Hauptleitung festgelegt auf der in regelmäßigen Abständen vorher festgelegte Hosts kontaktiert werden. Stellt das AddOn fest, dass die Server nicht erreichbar sind, geht es davon aus, dass die Hauptleitung ausgefallen ist. Nun rekonfiguriert LineTest die Internetverbindung und schaltet auf Ersatzleitung um. Entweder bleibt diese solange bestehen bis manuell wieder auf die Hauptleitung umgeschaltet, oder aber ein Cronjob überprüft in regelmäßigen Abständen, ob die Hauptleitung wieder verfügbar ist[18].

Obwohl der IPCop bereits ein ähnlich Funktion bereitstellt, eignet sich diese AddOn beim Einsatz mehrerer Verbindungsarten. IPCop erlaubt es nur zwischen definierten Einwahlprofilen zu wechseln. Ein automatische Umschaltung auf das erste Profil ist jedoch nicht vorgesehen. Zudem fällt diese Möglichkeit aus, sobald IPCop über eine statische IP-Adresse, über einen vorgelagerten DHCP Server oder über eine ISDN-Karte die Verbindung herstellt.

Installation Das AddOn wird installiert, indem das Paket auf den IPCop in ein temporärers Verzeichnis kopiert und dort mittels tar entpackt wird. Danach wird die Installation in entpackten Verzeichnis durch Eingabe des Befehles ./install gestartet. Die Installationsroutine erwartet nun ein Eingabe der Option, ob das Tool installiert oder ob es aktualisiert werden soll[15].

Konfiguration Nach der Installation wird mit dem Befehl *cd -L* ins root Verzeichnis gewechselt. Es müssen nun die Netzwerktypen für die Haupt- und Backupleitung definiert werden. Dazu wird zunächst über den Befehl *setup* das IPCop Konfigurationsprogramm gestartet. Im Bereich *Networking* wird nun der Typ für die Hauptverbindung festgelegt. Nachdem die Einstellung gespeichert und das Setup verlassen wurde, muss die Konfiguration durch den Befehl */var/IPCop/linetest/check.sh –saveprimary* gesichert werden. Die Auswahl der Backupleitung erfolgt auf identischer Art und Weise. Diese Konfiguration wird mit dem Befehl */var/IPCop/linetest/check.sh –savebackup* ebenfalls gesichert.

Als nächstes werden im Web-Frontend des IPCop die dazu passenden Einwahlprofile festgelegt. Anschließend werden die restlichen Einstellungen im LinTest AddOn im Menü *Netzwerk* vorgenommen. Hier werden die drei im Internet zu prüfenden Hosts eingetragen und in welchem Abstand die Prüfung vorgenommen werden soll. Zusätzlich kann ein sendmail Client aktiviert werden, der eine E-Mail versendet sobald das LineTest AddOn zum Einsatz kommt[15].

5.9 GUI-Ports

Das Tool GUI-Ports ist von Stephan Feddersen entwickelt worden. Da der Zugriff auf das Webfrontend des IPCops bereits auf andere Ports umgelegt wurde, http auf Port 81 und https auf Port 445 ist es möglicherweise notwendig diese Ports ebenfalls zu verlegen. Dazu richtet sich dieses AddOn seinen eigenen Bereich im Webfrontend unter System > Einstellungen in der Benutzeroberfläche ein. Dort kann der Benutzer die Ports für die beiden Protokolle auf andere Ports legen. Es empfiehlt sich diese in den Highport Bereich ab 1024 zu verlegen, da Sie dort nicht mit anderen Diensten in Konflikt kommen und diese bei PortScans seltener untersucht werden[13].

Installation Die Installation erfolgt durch Entpacken des Archivs in einem temporärem Ordner auf dem IPCop. Dort wird der Befehl *./install* im entpackten Ordner GUIports ausgeführt. Nach Durchlaufen der selbsterklärenden Installation steht dem Benutzer das AddOn im Webfrontend zur Verfügung[14].

Konfiguration Im Bereich der Einstellungen der Benutzeroberfläche können der HTTP-Port sowie der HTTPS-Port konfiguriert werden. Nach dem Drücken der Taste *Speichern und ändern* werden die neuen Ports sofort übernommen. Der Apache Webserver wird auf dem IPCop neu gestartet. Das Webfrontend muss danach über den neuen Port neu aufgerufen werden. Abbildung 5.9 zeigt die Konfiguration der GUI-Ports[14].

Einstellung der Benutzeroberflächen Ports
HTTP Port: 81
Der Standard HTTP Port des IPCops ist 81. Hier kann der Port angepasst werden!
HTTPS Port: 445
Der Standard HTTPS Port des IPCops ist 445. Hier kann der Port angepasst werden!
speichern und ändern
Anmerkung: Nach dem Drücken des Buttons "speichern und ändern" werden die hier gemachten Einstellungen sofort und ohne Neustart übernommen. Sollte der HTTPS Port geändert worden sein, wirkt sich dies auch auf das Aufrufen des IPCop Webinterfaces aus. Bitte nach dem Ändern des HTTPS Ports das Webinterface des IPCops mit den neuen Einstellungen neu aufrufen.
GUIPorts Ver: 1.6.2

Abbildung 5.9: Screenshot Konfigurationsmaske GUI-Ports

5.10 UPS

Das UPS-Server AddOn von Stephan Feddersen bietet eine grafische Auswertung des aktuellen Status einer angeschlossenen USV, Diagramme über den Verlauf der wichtigsten Daten zur USV und bietet darüber hinaus die Möglichkeit das System oder auch weitere Systeme via Remote sofern durch die USV unterstützt, bei einem Stromausfall herunterzufahren[19]. Nachteilig bleibt jedoch zu erwähnen, dass dieses AddOn nur mit unterbrechungsfreien Stromversorgungen der Firma APC zusammen arbeitet, da es auf dem Projekt Apcupsd, `http://www.apcupsd.com` aufbaut. Apcupsd ist der Daemon zur Kontrolle von unterbrechungsfreien Stromversorgungen der Firma APC auf dem dieses AddOn basiert. Die Abbildung 5.10 zeigt eine Zusammenfassung des AddOns von einer an den IPCop angeschlossenen unterbrechungsfreien Stromversorgung.

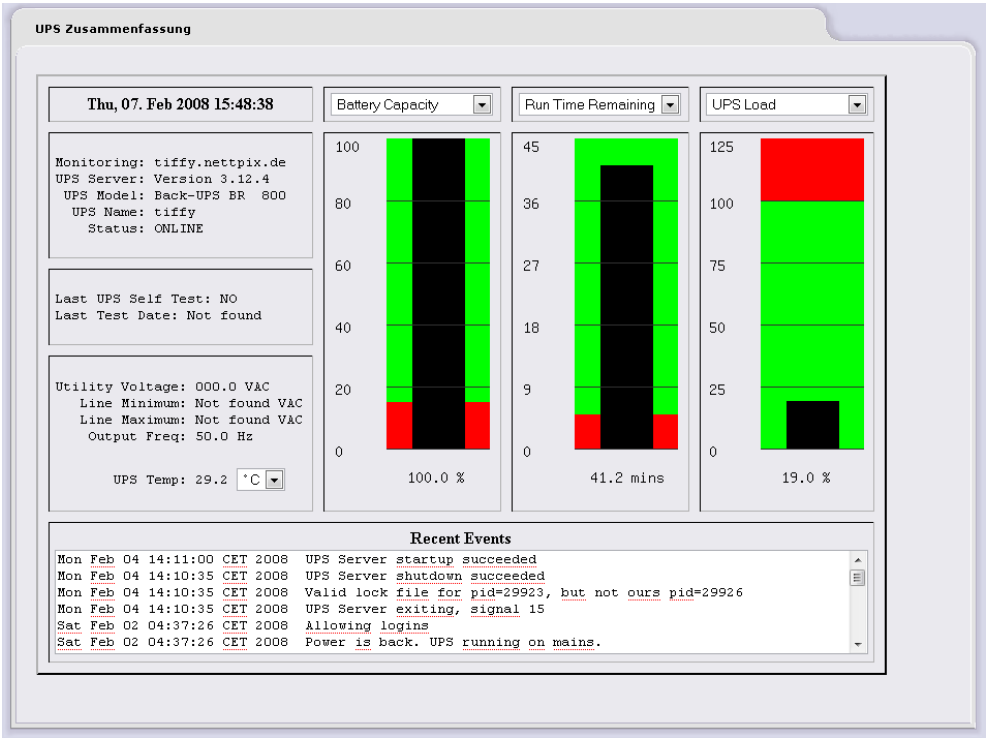

UPS Zusammenfassung
Thu, 07. Feb 2008 15:48:38
Battery Capacity
Run Time Remaining
UPS Load
Monitoring: tiffy.nettpix.de
UPS Server: Version 3.12.4
UPS Model: Back-UPS BR 800
UPS Name: tiffy
Status: ONLINE
Last UPS Self Test: NO
Last Test Date: Not found
Utility Voltage: 000.0 VAC
Line Minimum: Not found VAC
Line Maximum: Not found VAC
Output Freq: 50.0 Hz
UPS Temp: 29.2 °C
100.0 %
41.2 mins
19.0 %
Recent Events
Mon Feb 04 14:11:00 CET 2008 UPS Server startup succeeded
Mon Feb 04 14:10:35 CET 2008 UPS Server shutdown succeeded
Mon Feb 04 14:10:35 CET 2008 Valid lock file for pid=29923, but not ours pid=29926
Mon Feb 04 14:10:35 CET 2008 UPS Server exiting, signal 15
Sat Feb 02 04:37:26 CET 2008 Allowing logins
Sat Feb 02 04:37:26 CET 2008 Power is back. UPS running on mains.

Abbildung 5.10: Screenshot UPS Zusammenfassung

Installation Das Paket wird auf dem IPCop in ein temporäres Verzeichnis übertragen und dort mittels tar entpackt. Im daraufhin erstellten Verzeichnis wird die Installation durch Eingabe des Befehls *./install* gestartet. Nach erfolgtem Start erwartet die Installation die Auswahl einer Option, um das AddOn zu installieren. Es stehen die Optionen *smbclient*, *msgclient* und *sendmail* sowie eine Kombination der Optionen zur Verfügung. Bei der Auswahl des *smbclient* werden Nachrichten beim Einsetzen der USV per Nachrichtendienst versendet. Dazu muss unter Windows 2000/Windows XP der Nachrichtendienst aktiviert sein. Da seit dem SP2 von Windows XP der Nachrichtendienst deaktiviert ist, steht die Option *msgclient* zur Verfügung. Diese nutzt ein weiteres AddOn um Nachrichten über einen *msgclient* zu empfangen. Dieses muss dazu lokal auf dem Windowsclient installiert sein. Die letzte Option sendmail lässt sich mit den bereits erwähnten Optionen kombinieren. *Sendmail* sendet dabei die Nachricht an ein zuvor konfiguriertes Postfach. Nach Auswahl der bevorzugten Option verläuft die Installation automatisiert ab[16].

Konfiguration Das AddOn nimmt seinen Platz im Menü *Dienste* unter dem Punkt *UPS* ein. Um das AddOn zu aktiveren muss die Checkbox *UPS Server* aktivieren gesetzt werden. Dann bekommt die UPS einen Namen. Das Feld *Full Quallified Domain Name* (FQDN) wird benö-

tigt um eine erneute Anmeldung bei Ansicht der UPS Statusseite zu vermeiden. In dem Feld *Modus* kann ausgewählt werden, ob die USV allein stehend betrieben wird, oder ob Sie über eine Netzwerkverbindung angeschlossen wird. Als letztes muss noch der Typ der USV angegeben werden. Dieser muss mit der angeschlossenen USV übereinstimmen, da je nach Typ weitere Felder eingestellt werden müssen. Dies ist beispielsweise notwendig für die Art des Anschlusses der Firewall mit der USV. Dazu muss je nach Typ das verwendete Kabel und der jeweilige Anschlussport (COM oder USB) ausgewählt werden. Weiterhin können weitere Einstellungen zu Shutdown und Benachrichtigung eingestellt werden. Da bereits Standardwerte hinterlegt sind, können diese übernommen werden. Sind die Einstellungen getroffen, werden diese gespeichert. Danach wird der Dienst gestartet.

Um im Fall des Einsatzes der USV eine Nachricht an den zuständigen Administrator zu senden, muss die verwendete Option aktiviert werden. Es stehen dazu nur die Optionen zur Verfügung, die bei der Installation ausgewählt wurden. Dazu muss je nach Typ des Nachrichtendienst dieser konfiguriert werden. Im Fall durch Benachrichtigung via E-Mail durch Eingabe des verwendeten E-Mailservers inklusive der Daten der Absender und Empfänger sowie der Daten SMTP Authentifizierung bei Verwendung der *Sendmail* Option. Bei den beiden Nachrichtendiensten muss der empfangende Client angegeben werden[16].

Das AddOn wird ist mit einer Online-Hilfe ausgestattet.

5.11 SystemInfo

SysInfo stellt in der WebGUI erweiterte Informationen zum verwendeten System dar. Angezeigt werden Informationen zu CPU und zur Systemfestplatte, zu den PCI-Geräten, den Netzwerkkarten und den angeschlossenen USB-Geräten. Zusätzlich werden die Interrupts dargestellt und das BIOS wird ausgelesen. Weiterhin werden ähnlich dem Befehl Top die laufenden Prozesse angezeigt. Somit gibt SysInfo einen schnellen Überblcik über das System ohne sich diese Informationen über ein ShellConsole ausgeben zu lassen[12].

Installation Nachdem das heruntergeladene Paket auf den IPCop übertragen wurde, wird dieses in einem temporärem Verzeichnis mit tar entpackt und durch die Eingabe des Befehls *./install -i* installiert. Die Installation verläuft ohne weitere Nachfrage automatisiert ab.

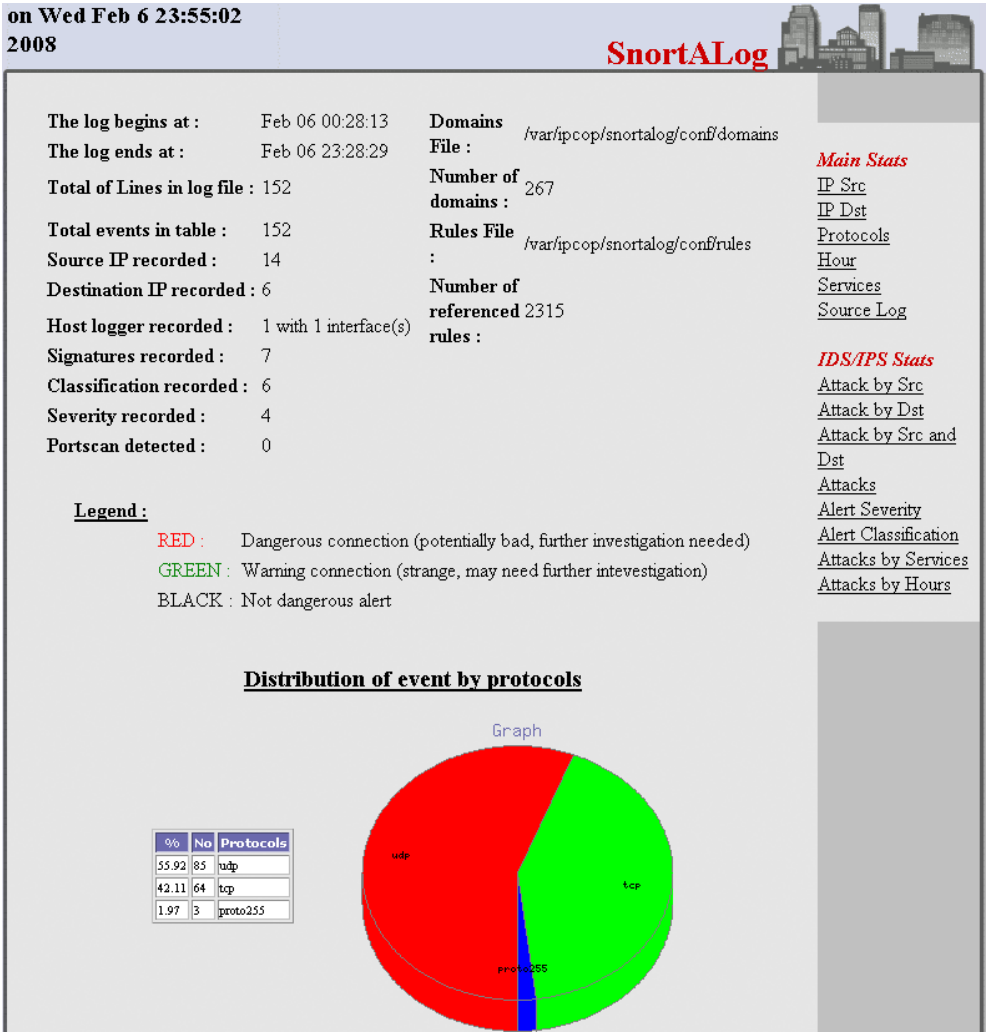


Abbildung 5.11: Screenshot Bericht des AddOns SnortALog

Konfiguration Eine Konfiguration dieses AddOns ist nicht erforderlich.

5.12 SnortALog

Da ein aktives Intrusion Detection System nur nützlich sein kann, wenn die Logdatei gründlich ausgewertet wird, empfiehlt es sich dazu das AddOn SnortALog zu installieren. Dieses AddOn erstellt täglich einen Bericht über die Einträge aus dem Log von Snort. Der Bericht, siehe Abbildung 5.11, beginnt mit einer Übersicht und Zusammenfassung verschiedener Punkte.

Dazu gehören unter anderem Start- und Endzeitpunkt des Logs, Anzahl der Ereignisse im Log,

Anzahl unterschiedlicher Quell- und Ziel-IP-Adressen und einer Übersicht über den aktuellen Regelstatus von Snort. Danach erfolgen grafische Darstellungen über die prozentuale Verteilung der angegriffenen Protokolle (udp,tcp,icmp...), prozentuale Verteilung des Schweregrads, zeitliches Auftreten des Angriffs (Anzahl, prozentuale Verteilung und Schweregrads) und prozentuale Verteilung der angegriffenen Ports. Danach erfolgt die tabellarische Darstellung aller aufgetretenen Ereignisse[24].

Das SnortALog AddOn wurde von Markus Hoffmann entwickelt und basiert auf das Perl Script SnortALog von Jérémy Chartier[8].

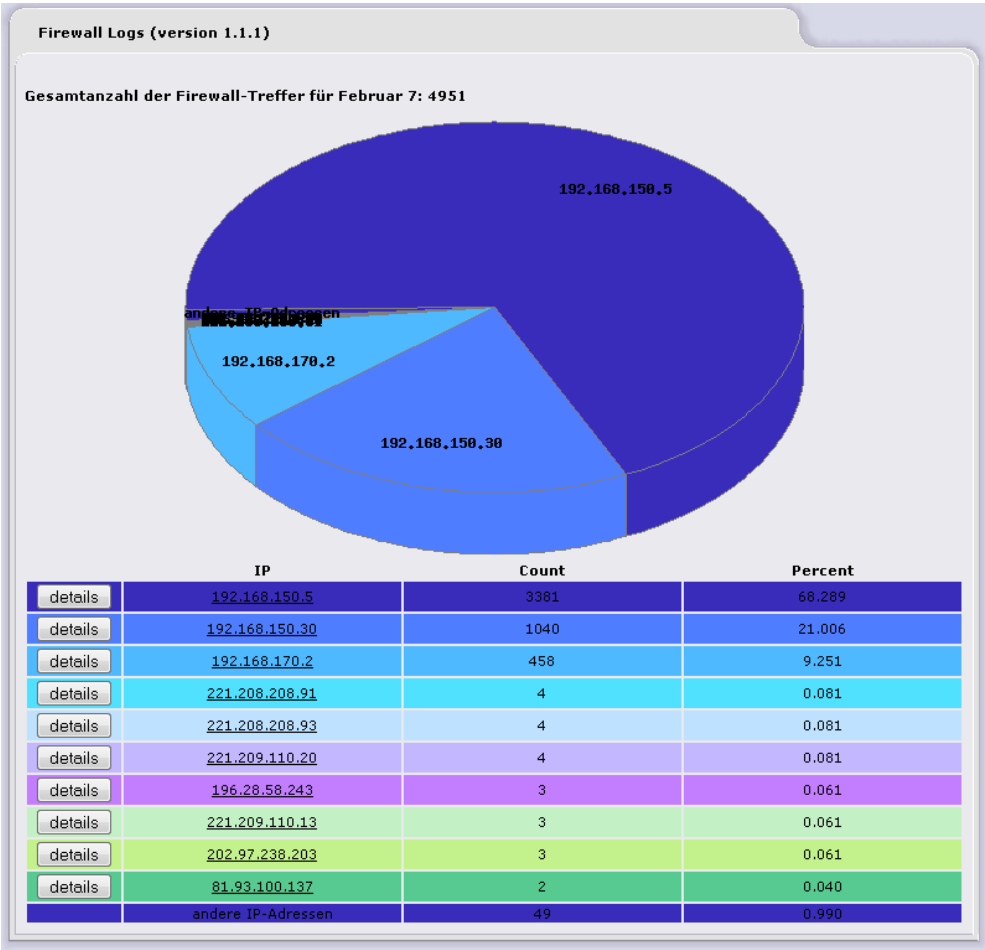
Installation Das heruntergeladenen AddOn wird auf den IPCop in ein temporäres Verzeichnis kopiert. Danach wird dieses mit tar entpackt und im danach erstellten Ordner die Installation durch Eingabe des Befehls *./install* gestartet. Die Installation läuft automatisch und ohne weitere Nachfragen ab.

Konfiguration Nach der Installation kann SnortALog im Webbrowser über den Menüpunkt *Logs* > *SnortALog* aufgerufen werden. Wird SnortALog über den Haken *Enable SnortALog* aktiviert, werden täglich neue Berichte generiert. Diese können im Webbroser aufgerufen werden. Alternativ besteht die Möglichkeit die Berichte nach der Generierung automatisiert an eine E-Mail-Adresse zu versenden.

5.13 FireWall Logs

Firewalllogs ist ein weiteres AddOn von Markus Hofmann und erweitert die Auswertung des Firewall Logs um eine grafische Komponente. Alle Treffer der Firewall, die im Log festgehalten wurden, werden mit diesem Tool in einer Tortengrafik dargestellt. Siehe dazu Abbildung 5.12.

Dies erfolgt wahlweise nach Quell-IP oder nach betroffenem Port. Zudem hat dieses AddOn den Vorteil, dass die tabellarische Ansicht des Firewall Logs um eine Filteroption erweitert wurde. So können etwa alle Einträge im Firewall Log gefiltert nach IP oder Port aufgelistet werden. Dies erleichtert zum einen die Suche nach einem Fehler bei der Konfiguration neuer Dienste im Netz, aber auch die Überprüfung der Angriffe auf das eigene Netz. Die Installation verläuft ohne weitere Nachfrage automatisiert ab[34].



	IP	Count	Percent
details	192.168.150.5	3381	68.289
details	192.168.150.30	1040	21.006
details	192.168.170.2	458	9.251
details	221.208.208.91	4	0.081
details	221.208.208.93	4	0.081
details	221.209.110.20	4	0.081
details	196.28.58.243	3	0.061
details	221.209.110.13	3	0.061
details	202.97.238.203	3	0.061
details	81.93.100.137	2	0.040
	andere IP-Adressen	49	0.990

Abbildung 5.12: Screenshot Bericht des AddOns Firewall Logs

Installation Das auf den IPCop übertragene Paket wird mit tar entpackt und anschließend durch Eingabe von *./install* gestartet. Die neuen Firewalllogs sind dann im Webinterface im Menü *Logs* erreichbar.

Konfiguration Eine Konfiguration dieses AddOns ist nicht erforderlich.

5.14 RootkitHunter

RootkitHunter ist ebenfalls ein von Markus Hofmann entwickeltes AddOn. Es basiert auf dem OpenSource Projekt rkhunter. Rkhunter ist ein Unix basierendes Tool, welches das System nach rootkits, backdoors und möglichen Exploits untersucht, indem es von den wichtigsten

Dateien MD5-Hashes bildet und diese mit einer Online-Datenbank vergleicht[26]. Die Installation im IPCop richtet zudem einen Cronjob ein, der täglich den Rootkit Hunter aktualisiert und ausführt.

Installation Nach Download des Pakets wird dieses in ein temporäres Verzeichnis verschoben und dort mit tar entpackt. Danach wird das Installationsscript *./installer.sh* im erstellten Verzeichnis gestartet. Die Installation läuft automatisiert ab und verlangt keine weiteren Eingaben[23].

Konfiguration Rootkit Hunter richtet sich im Menü *Dienste* als neuen Punkt *RootKitHunter* ein. Eine Konfiguration ist nicht erforderlich. Es ist lediglich möglich auf Knopfdruck das AddOn zu aktualisieren beziehungsweise einen Check des Systems manuell zu starten

5.15 Coptime

Ein für den produktiven Einsatz weniger empfohlenes AddOn ist CopTime. Der Einsatz empfiehlt sich nicht, da es keinen sicherheitsrelevanten Zweck oder Nutzen erfüllt und wie eingangs erwähnt jedes zusätzliche Stück Software ein zusätzliches Risiko für die Firewall birgt. Gerade aber mit diesem AddOn, kann die Stabilität des Systems dargestellt werden.

CopTime ist ein Dienst, der im zweistündigen Rhythmus Daten der bisherigen Laufzeit des Systems seit dem letzten Neustart an eine Datenbank der Webseite des IPCop Forums überträgt, `http://www.ipcop-forum.de/coptime`. Auf dieser Webseite werden alle am Dienst teilnehmenden Firewall-Systeme in einem Ranking dargestellt. Zum Zeitpunkt der Erstellung dieser Arbeit sind ca. 600 aktive System aufgeführt. Eine detaillierte Bewertung dieses Dienstes wird im Kapitel 5.2 aufgeführt.

Installation Die Installation gestaltet sich folgendermaßen. Das Paket wird mittels einer Remote Console auf die Firwall übertragen und dort in einem temporärem Verzeichnis entpackt. Die Installation wird als nächstes im erstellten Verzeichnis durch Eingabe von *./install* gestartet[62]. (Das AddOn sowie die Dokumentation sind nur erhältlich sofern eine Mitgliedschaft im IPCop-Forum existiert)

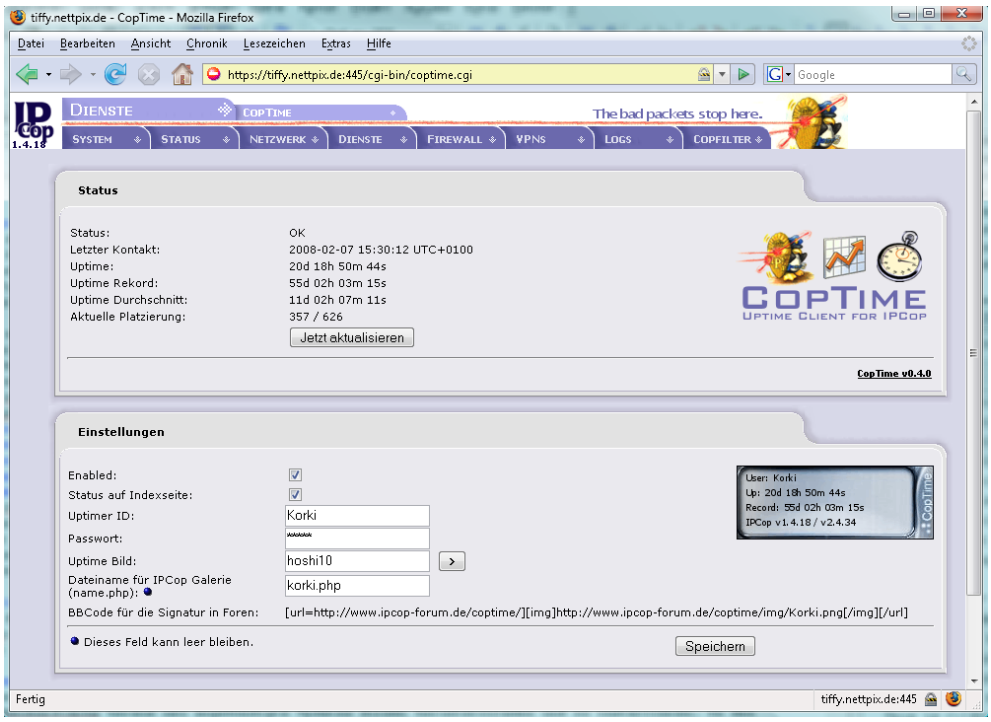


Abbildung 5.13: Screenshot Konfigurationsmaske Coptime

Konfiguration Nach erfolgter Installation befindet sich im Menü *Dienste* des IPCops ein weiterer Menüpunkt *Coptime*. Zur Aktivierung des Dienstes wird ein Haken bei enabled gesetzt. Zusätzlich ist eine Mitgliedschaft im Forum der bereitstellenden Webseite erforderlich. Der Forumsname wird im Feld Uptimer ID eingetragen. Bei der ersten Einrichtung kann ein frei wählbares Kennwort gewählt werden. Dieses wird bei der ersten Übertragung dauerhaft in der Datenbank gespeichert. Zuletzt wird ein beliebiges Hintergrundbild gewählt. Dieses kann zum Beispiel als Signatur bei aktiver Teilnahme am Forum verwendet werden, wird aber auch auf der Seite des Coptime-Dienstes angezeigt. In Abbildung 5.13 ist die Konfigurationsmake von Coptime dargestellt[62].

6 Wartung und Pflege

Mit einer Installation einer Firewall alleine ist es in der Regel nicht getan. Wie bereits erwähnt, ist eine Firewall Teil eines Gesamtkonzeptes zur Absicherung des Netzwerks auf ein- und ausgehenden Datenverkehr. Zum Gesamtkonzept gehört auch eine regelmäßige Kontrolle der Firewall. Dies umfasst mehrere Bereiche. Zum einen müssen regelmäßig die Logdateien geprüft werden. Diese sind abhängig von den installierten Komponenten. Es müssen in jedem Fall die Firewalllogdateien überprüft werden sowie die gesamten Logdateien der Firewall. Dazu gehören berichte über Cronjobs, Kernellogs, Logins, und SSH-Verbindungen. Aber auch, je nach aktiviertem Dienst und installiertem AddOn, Einsicht in die Proxyberichte, Überprüfung der Snortlogs oder des DHCP-Servers. Auch sollte bei der jetzigen Frequenz der Updates mindestens einmal im Monat die Prüfung auf Aktualisierungen für den IPCop vorgenommen werden. Sofern AddOns installiert sind, ist es ratsam dies auch auf Aktualisierungen innerhalb der jeweiligen AddOns vorzunehmen.

6.1 Updates

Zur regelmäßigen Pflege gehört das Einspielen neuer Updates, sofern welche neu veröffentlicht werden. IPCop ist derzeit bei der Version 1.4.18 angelangt, welche Anfang Dezember 2007 veröffentlicht wurde. Momentan ist jedoch nicht davon auszugehen, dass in kürzeren Abständen neue Updates herauskommen werden. Der letzte Versionssprung dauerte bereits fünf Monate, die beiden davor jeweils drei Monate.

Die derzeitige RoadMap[64] des IPCops sieht für die Version 1.4.x nur noch zwei weitere geplante Updates vor. Zum einen die Aktualisierung auf Version 1.4.19, dann auf 1.4.20. Die geplanten Neuerungen werden dann folgende sein:

- 3G USB Serial Modem Unterstützung über dass Webfrontend
- Netzwerktreiber (skge und sky2)

- snort rules selector
- kernel 2.4.35
- Weitere WLAN-Treiber

Jedes weitere Update, dass nach 1.4.20 erscheint, wird ausschließlich Sicherheitslücken schließen und Bugs beheben. Es werden keine weiteren Funktionen hinzugefügt.

Nichts desto trotz ist bereits die Version 2.0 in Planung und Arbeit. Diese hat jedoch noch nicht einmal einen Alpha Status erreicht. Ein Termin für die Veröffentlichung ist weder bekannt noch geplant. Die Neuerungen werden folgende sein[64]:

- Kernel Version 2.6 (Hauptsächlich zur Unterstützung neuer Hardware)
- Neues WebGUI
- OpenVPN
- Unterstützung für Alpha, Power PC and Sparc Architekturen
- Eventuell weitere Funktionalitäten aus der nächsten Liste

Mittel- und langfrisitge Ziele[64]:

- Unterstützung mehrerer Schnittstellen (mehr als eine rote, orange, grüne)
- Neues Installationsprogramm
- Modulare Pakete unterschieden nach Test und Stabil
- Automatische Updates
- Bessere Unterstützung bei Flash-Medien
- Stärkere Übersetzung
- Weitere bereits integrierte AddOns (BOT, adv proxy, URL filter, und weitere ...)
- Neue Bootscripts (Linux from Scratch)
- WLAN-Support
- QoS kernel
- layer7 filter
- Firewall Schnittstelle basierend auf Shorewall (incl. QoS, etc.)
- Erster XML/RPC Daemon zur Konfiguration
- Vollständiges XML/RPC Management

6.2 Logauswertung

Bevor die Logauswertung vorgenommen werden sollte, ist es hilfreich die Einstellungen vorher für die Logdateien zu bearbeiten. In der Standardeinstellung werden die Logs in aufsteigender chronologischer Reihenfolge ausgegeben. Bequemer ist jedoch die umgekehrte chronologisch absteigende Ausgabe der Logs, da in der Ansicht immer nur jeweils eine Seite vor oder zurück geblättert werden kann. Zwar lässt sich die Ausgabe durch Manipulation des URLs beeinflussen, dies gleicht jedoch einem Ratesuchspiel. Ebenfalls lässt sich die Anzahl der Zeilen einstellen, um nicht ständig blättern zu müssen, da die unterschiedlichen Logs pro Tag mehrere tausend Einträge haben können. In diesem Zusammenhang ist es ebenfalls wichtig die Dauer für das Aufheben der Logs einzustellen. Es können durchaus einige Gigabytes an Daten zusammen kommen und je nach Größe der verwendeten Festplatte kann diese vollaufen. Dies gilt ebenso für den Detailierungsgrad.

Wer einen Syslog Server für Remotelogging betreibt kann diesen ebenfalls dazu verwenden die Logs des IPCops auf diesem zu speichern. Dazu ist es nötig das Remotelogging zu aktivieren und den Syslog Server namentlich anzugeben. Die Beschreibung zur Konfiguration ist jedoch weder in der deutschen noch in der englischen Dokumentation vorhanden.

Prinzipiell gibt es zwei Logs die sicherheitsrelevante Aufzeichnungen beinhalten. Zum einen gibt es die Firewalllogs. Die Einträge, die sich hier drin befinden, zeigen Verbindungsversuche zum Netzwerk, die jedoch von der Firewall nicht durchgelassen wurden. An diesen Logs lässt sich also feststellen, welche potentiellen Angriffe auf das Netzwerk durchgeführt wurden. Dabei muss ein solcher Eintrag jedoch noch nicht bedeuten, dass das Netzwerk gezielt angegriffen wurde. Viele Einträge können verursacht werden durch Tippfehler oder fehlerhaft konfigurierte Geräte. Allerdings sind die Firewalllogs auch in umgekehrter Weise hilfreich. So werden hier auch die Vorgänge protokolliert, die dazu Vorgesehen sind durch durch die Firewall zu gehen, jedoch geblockt werden. Der Administrator kann erkennen warum zum Beispiel ein Dienst nicht funktioniert und ob dieser von der Firewall geblockt wird[37, Kapitel 2.8.5].

Bei aktiviertem IDS ist das dafür vorgesehene Log ebenfalls eine Stelle, an der sich sicherheitsrelevante Vorgänge beobachten lassen. Wie jedoch im Kapitel über IDS bereits erwähnt lassen sich hier nur bekannte Vorgänge beobachten. Trotzdem lässt sich somit erkennen, welche Dienste angegriffen werden können sofern sich der jeweilige Dienst überhaupt im Netzwerk befindet[37, Kapitel 2.8.6].

Relevante Einträge für den Systemstatus einiger laufender Dienste können im Menüpunkt System-Logdateien eingesehen werden. Folgende Dienste und Funktion werden geloggt sofern diese aktiviert sind:

- NTP
- DNS
- Aktualisieren
- IPSec
- SSH
- Snort
- Login/Logout
- IPCop
- Cron
- Kernel
- RED
- DHCP-Server

Alternativ lassen sich die Logs auch über eine direkte Verbindung über ssh einsehen. Alle Logdateien werden auf dem IPCop im Verzeichnis */var/log* abgelegt. Auch die AddOns legen in der Regel hier ihre Logdateien ab. Über diesen Weg können die Logdateien auch gesichert werden. Sie brauchen allerdings nicht komprimiert werden, da die Logdateien bereits durch eine Rotation wöchentlich komprimiert werden. Nur die aktiven Logdateien werden im Textformat gespeichert.

6.3 Stabilität

Durch den Einsatz des AddOns Coptime wird deutlich wie sich die Stabilität des IPCops darstellt. Der Einsatz des AddOns Coptime wurde bereits in Kapitel „Weitere Funktionen und Dienste“ beschrieben. Die Auswertung der gesammelten Daten erfolgt auf der Seite des IPCop-Forums im Bereich Coptime. Hier ist in einem Ranking tabellarisch dargestellt, wer welche aktuelle Uptime hat, wie sein persönlicher Schnitt ist und was sein Maximum war. Derzeit haben rund 150 Benutzer eine Uptime von mehr als 100 Tagen, die Top 20 hat sogar eine Uptime von mehr als 300 Tage. Die Spitzenposition wird mit einer Uptime von über 350 Tagen bestritten. Tatsächlich sind es sogar noch einige mehr, wenn die Berücksichtigung des aktuellen Updates außer Betracht gelassen wird. Diese Zahlen und Diagramme zeigen

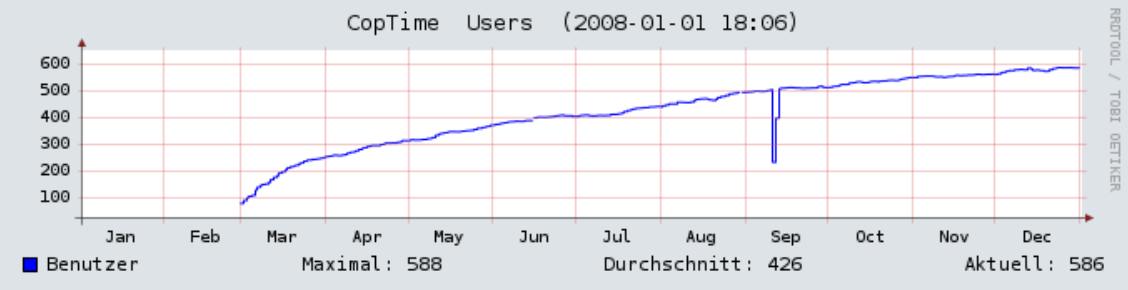


Abbildung 6.1: Anzahl der CopTime User - Jahresansicht[59]

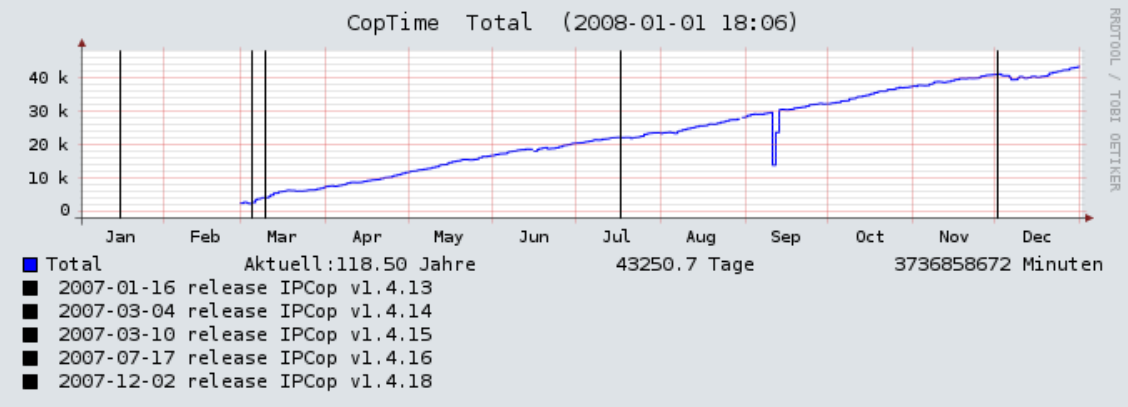


Abbildung 6.2: Uptimesumme aller User - Jahresansicht[61]

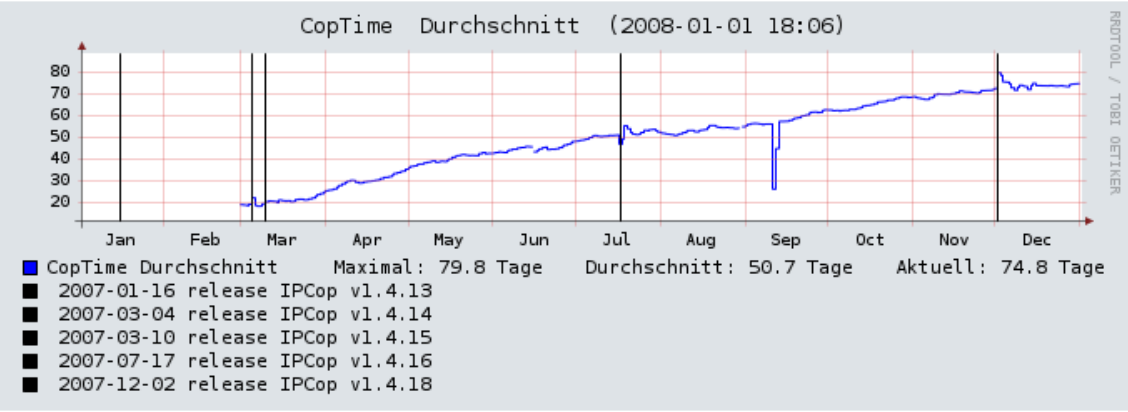


Abbildung 6.3: Durchschnittliche Uptime aller User - Jahresansicht[60]

deutlich wie Stabil der unterbrechungsfreie Betrieb der Firewall IPCop ist. Ein Reboot ist nur in den seltensten Fällen notwendig, etwa wenn ein AddOn installiert wird, welches tief eingreifende Änderungen im System vornimmt oder nach einem Update, welches einen Kernelwechsel durchführt. Der Spitzeneinbruch Mitte September und der minimale Einbruch Anfang Dezember zeigen jeweils einen Versionssprung.

6.4 Hilfestellung und Ressourcen

IPCop ist mittlerweile sehr bekannt und kann auf eine große und starke Community im Internet bauen. So gibt es zum einen die IPCop Projektseite: `http://www.ipcop.org`. Diese bietet auf internationaler Ebene neben der Möglichkeit IPCop und diverse Updates als Paket herunterzuladen zusätzliche Informationen. Dazu gehören unter anderem Handbücher zur Installation und Administration, FAQ-Seiten und Mail-Listen für den Support und Pressebereichte. Daneben gibt es auch Material über den Stand der Entwicklung und wie es möglich, ist sich an der Entwicklung zu beteiligen.

Auf nationaler Ebene gibt es gleich mehrere gute Quellen um Hilfe bei Problemen zu erhalten. Zum einen gibt das IPCop-Wiki: `http://www.ipcopwiki.de`. Hier wird eine deutsche Online-Dokumentation aufgebaut, die eine Sammlung allen erhältlichen Materials für den IPCop bereitstellt. Da die Gründung erst im Jahr 2006 war und sich noch nicht so viele an diesem Projekt beteiligen, sind noch nicht alle Beiträge vollständig. Auch fehlen einige Themen gänzlich. Trotzdem ist dies eine gute Quelle bei offenen Fragen.

Etwas bekannter ist das deutsche Forum zum IPCop, `http://www.ipcop-forum.de`. Diesem Forum sind derzeit über 10000 Mitglieder angeschlossen, und es sind bereits über 160.000 Beiträge geschrieben worden. Das Forum ist gut besucht, was sicherlich auch an den qualifizierten Beiträgen des Forums liegt. Der wichtigste Bereich auf dieser Seite ist sicherlich das gut strukturierte Forum selbst.

Neben allgemeinen Informationen und Verhaltensregeln gibt es in diesem Forum Bereiche zu Themen die der Tabelle 6.1 entnommen werden können.

Neben dem Forum gibt es noch weitere Bereiche. Zum einen gibt es eine Galerie mit Abbildungen über die eingesetzte Hardware einiger User. Weiterhin befinden sich hier die deutsche Dokumentation sowie auch die einzelnen IPCop Pakete zur Installation und auch Updates für

Tabelle 6.1: Übersicht Foren Bereiche

Forenbereich	**Inhalt**
1.4.x IPCop generell	Allgemeines zu IPCop
1.4.x IPCop Installation & Updates	Alles zur Grundinstallation von IPCop und alles zu den Updates
1.4.x IPCop Konfiguration & Administration	Alles was mit der Konfiguration von IPCop und den Clients zu tun hat
1.4.x IPCop Addons & Modifikationen	Addons, Modifikationen und zusätzliche Software für IPCop
1.4.x IPCop und Hardware	Bei Problemen mit IPCop und Hardware, Hardwareanforderungen von IPCop
1.4.x IPCop und Server	Serverfarm hinter IPCop? Einstellungen/Konfiguration, welche Ports
1.4.x IPCop und VPN	VPN Allgemein, VPN Roadwarrior, VPN IPCop-IPCop, OpenVPN
1.4.x IPCop und WebProxy	WebProxy und IPCop, Advanced Proxy, URL-Filter, Update-Accelerator
1.4.x Only for english speakers	IPCop related discussions in english (all topics)
IPCop Alpha/Beta/Testversionen generelles	Allgemeines zu Testversionen, Hard- und Software Probleme
IPCop, alte Versionen, alle Themen	Alle Themenbereiche, nur ältere IPCop Versionen (Nur-Lese-Archiv)
Verschieden weitere Bereiche zu Computer und Sicherheit	

ältere Versionen auf dieser Seite. Das IPCop-Forum beinhaltet zudem auch die Präsenz für das AddOn CopTime, welches sich in einem unterteilten Bereich befindet.

Eine weitere Seite, `http://www.ipcopaddons.org` erstellt von Torben Boockmann einem Mitglied des IPCop Forums, ist eine AddOn Datenbank die seit Oktober 2007 im Netz erreichbar ist. Hier befindet sich ein Großteil der AddOns, die für den IPCop entwickelt wurden mit einer kurzen prägnanten Beschreibung des jeweiligen AddOns. Auf der Seite sind die AddOns zur einfachen Suche unterteilt in mehrere Bereiche:

- Proxy
- VPN
- Logging
- Utilities

- Server
- Traffic

Auf der Seite sind die Downloads nicht direkt hinterlegt sondern verweisen lediglich auf die Seite des jeweiligen Entwicklers. Dennoch ist diese Datenbank hilfreich, da alle AddOns an zentraler Stelle zusammengefasst sind.

Ein weiterer Anlaufpunkt sind folgende Seiten:

- `http://www.ipadd.de` (Tom Eichstaedt)
- `http://mh-lantech.css-hamburg.de` (Markus Hoffmann)
- `http://www.h-loit.de` (Stephan Feddersen)
- `http://www.ban-solms.de` (Olaf Westrik)
- `http://ipcop.gutzeit.ch` (Eckart Gutzeit)

Diese Seiten werden ebenfalls je von einem Mitglied des IPCop-Forums betrieben. Die Betreiber sind allesamt AddOn-Entwickler. Sie bieten auf Ihren Seiten Informationen zum IPCop, aber vor allem auch zu Ihren eigenen entwickelten AddOns Hilfestellung zu Installation, Konfiguration und Betrieb dieser.

7 Zusammenfassung

In der heutigen Zeit ist der Einsatz einer Firewall unumgänglich. Nahezu jeder, der einen Computer hat, ist mit diesem in der Regel auch online. Nach einer Studie des Verbands BITKOM haben 70 Prozent aller Bundeshaushalte einen PC. 50 Prozent der Haushalte haben einen Breitbandanschluss für den Zugang zum Internet und 67 Prozent haben eine E-Mailadresse[7]. In Unternehmen ist der Zugang sogar unvermeidlich, da die meisten Geschäftsmodelle die Einbeziehung des Internets voraussetzt. Mindestens basiert jedoch die tägliche Korrespondenz auf einen Zugang zum Netz.

Der Verzicht auf den Einsatz einer Firewall ist vergleichbar mit russischem Roulette oder einem Haus in dem Türen und Fenster offen stehen. Also eine Einladung für jedermann dort einen Besuch abzuhalten um sich mal um zuschauen was es dort alles gibt und für den Besucher von Interesse sein könnte. Im privaten Umfeld ist dies für den Einzelnen sicherlich unangenehm. Wenn allerdings ein Unternehmen einen Fremden, einen Kunden oder gar einen Mitarbeiter auf dieser Art und Weise bittet, sich im Unternehmen genauer zu informieren ist dies für den Geschäftsführer und seine Angestellten schon kritisch und könnte existenzielle Konsequenzen mit sich bringen.

Von allgemeinem Interesse ist es jedoch dann, wenn jedermann sich bei Krankenkassen, Banken oder staatlichen Institutionen Informationen über andere Personen besorgen kann (Kontostände, Lebensverhältnisse, persönliche Daten). Das alles sollte schon Grund genug sein eine Firewall einzusetzen.

IPCop ist ein Mittel der Wahl. Es ist kein Allheilmittel, aber gut genug um schnell, effektiv und zuverlässig seine Daten im Netzwerk zu schützen. Durch den Einsatz einer Firewall darf sich der Benutzer jedoch nicht in Sicherheit wiegen, denn diese kann trügerisch sein. Wie eingangs gezeigt gehört zu einem sicheren Netzwerk nicht nur eine Firewall, denn die meisten Angriffe finden bereits innerhalb des eigenen Netzwerkes statt. Gefahren lauern auf USB-Sticks, befinden sich in Softwarefehlern oder gar in der Inkompetenz oder Unwissenheit des Anwenders selbst.

Sobald IPCop an einem Zugangspunkt zum Internet installiert ist, ist bereits das dahinter liegende Netzwerk vor Angriffen aus dem Internet geschützt. Mit den gezeigten Funktionen und Diensten lässt sich eine komplexe Infrastruktur aufbauen, die einfach zu administrieren und leicht wartbar bleibt.

Durch den Einsatz weiterer AddOns lassen sich Administration und Wartung (etwa am Beispiel zur Auswertung der Log-Dateien) weiter vereinfachen. Auch können diese dazu dienen IPCop um weitere Funktionen zu ergänzen wie dies etwa die AddOns Advanced Proxy, URLfilter oder Tools zur Erweiterung der Benutzeroberfläche zeigen. Letztlich lässt sich IPCop noch mit einigen AddOns schärfer einstellen und trägt somit zu zusätzlicher Sicherheit bei. Das AddOn BOT etwa in dem es generell alle Verbindungen sperrt und gewollte Verbindungen manuell anhand von Regeln definiert werden müssen. Aber auch mit Copfilter, der ein komplettes Paket an Tools mit sich bringt und auf dem IPCop unter anderem ein E-Mail-Relay erstellt, welches Viren- Spam- und Phishingfilter enthalten.

Die Tabelle 7.1 dient der übersichtlichen Anschauung über den Funktionsumfang und Nutzen des jeweiligen AddOns. Die Anzahl der Sterne repräsentiert dabei den jeweiligen Funktionsgewinn.

Die Voraussetzungen zur Nutzung des IPCop sind so gering, das die Anschaffung neuer Hardware in der Regel ausbleiben kann. Die Kosten für die Hardware liegen bei unter hundert Euro sofern keine neue Hardware angeschafft werden muss. Die Einarbeitung und Installation ist innerhalb eines Tages abgeschlossen, und für die Wartung und Auswertung der Logs können ungefähr 20 Minuten am Tag veranschlagt werden, was einem wöchentlichem Aufwand von zwei Stunden entspricht. Die Kosten für den Betrieb sind demnach überschaubar.

IPCop kann als flexible und kostengünstige Alternative zu hochpreisigen Firewallsystemen konkurrieren. Der Einsatz in kleinen bis mittelständichen Unternehmen zur Absicherung des Netzwerks wird empfohlen.

Tabelle 7.1: Übersicht Addons - Funktionsumfang/Nutzen

AddOn	**Proxy**	**Performance**	**Sicherheit**	**Stabilität**	**Logging**	**Bemerkung**
Quality of Service		**		*	*	Bandbreiten-reglementierung
BlockoutTraffic			***		*	Traffic-reglementierung
Advanced Proxy	***	***	**		*	Umfangreicher Proxy
Update Accelerator	*	**			*	Zwischenspeicher für große Downloads
Calamaris					***	Proxylog-Analyse
URL-Filter			**			Blocken nichterwünschter Webseiten
Copfilter	**		***		***	SPAM-/Virenfilter
Ucarp				***		Überprüfung des Verfügbarkeit
Webalizer					**	Proxylog-Analyse
Line-Test				***		Überprüfung des Verbindungsstatus
GUI-Ports			*			Änderung der Standard IPCop Ports
UPS				**	*	Überprüfung der Stromversorgung
SystemInfo				*	**	System-Analyse
SnortALog			*		**	Log-Analyse
FirewallLog			**		**	Log-Analyse
RootKitHunter			**			Untersuchung auf RootKits
Coptime				*	**	Auswertung der Stabilität

Glossar

ACK Das ACK-Flag steht für die Empfangsbestätigung einer TCP-Verbindung[30], S. 8.

AddOns Programme zur Erweiterung einer Software um weitere Funktionen, S. 2.

ARP Address Resolution Protocol zur Umsetzung von Hardwareadressen zu Netzwerkadressen, MAC-Adresse <-> IP-Adresse[30], S. 7.

Bundestrojaner Umgangssprachliche Bezeichnung einer staatlich durchgeführten Online-Durchsuchung, S. 5.

Community Zusammenschluss einer Gruppe von Personen innerhalb des Internets die sich überwiegend mit einem Thema im Schwerpunkt beschäftigen und sich dazu austauschen, S. II.

DHCP Dynamic Host Configuration Protocol zur automatischen Einrichtung von Computern in Netzwerken[9], S. 2.

DNS Domain Name Service zur Übersetzung von Hostname zu IP-Adresse[30], S. 7.

DoS Ein Denial of Service hat das Ziel einen Rechner insofern zu kompromittieren, das dieser seinen geplanten Einsatz nicht mehr erfüllt[52], S. 5.

EICAR Von der European Expert Group for IT-Security EICAR entwickeltes Testmuster zur Überprüfung von Antivirenprogrammen, S. 65.

Exploit Sicherheitslücke aufgrund eines Programmierfehler in einer Software[52], S. 4.

false negatives Fehlerhaftes erkennen einer SPAM Nachricht.[10], S. 62.

false positives Fehlerhaftes erkennen einer erwünschten Nachricht.[10], S. 62.

FTP File Transfer Protocol zur Übertragung von Dateien in einem Netzwerk welches standardmäßig auf Port 21 betrieben wird[30], S. 10.

Gateway Zentrale Vermittlungsstelle in Rechnernetzwerken. Ein Router übernimmt in vielen Fällen die Funktion des Standardgateways, S. 1.

GUI Das Graphical User Interface ist die Schnittstelle zwischen Mensch und Maschine, S. 48.

HTTP Hypertext Transfer Protocol zur Übertragung von Daten in einem Netzwerk welches standardmäßig auf Port 80 betrieben wird[30], S. 10.

iptables Iptables ist die Weiterentwicklung des ursprünglichen Paketfilter ipchains. Es erlaubt die Definition von Regeln in Tabellen die aus mehreren Ketten bestehen die an Netfilter weitergegeben werden[52], S. 9.

LDAP Lightweight Directory Access Protocol ist ein Abfrageprotokoll für Verzeichnisdienste, S. 46.

MAC Die Media Access Control dient der eindeutigen Identifizierung von Geräten in einem Netzwerk[30], S. 7.

MIME Multipurpose Internet Mail Extensions dient zur Ermittlung des übermittelten Datentyps und Festlegung der Zeichenkodierung der Übertragung.[11], S. 46.

Proxies Ein stellt im Auftrag eines anderen Clients eine Verbindung her. Er speichert zudem den Internetdatenverkehr zwichen um ihn später bei erneuter Anforderung schneller ausliefern zu können[52], S. 4.

RADIUS Remote Authentification Dial-In User Service ist ein Protokoll zur Authentifizierung von Benutzern bei Verbindungen im Netzwerk., S. 46.

RDP Remote Desktop Protokoll zum Betrieb von Terminaldiensten in einem Netzwerk zwischen zwei Rechnern, S. 15.

SMTP Simple Mail Transfer Protokol zum Austausch von E-Mails zwischen E-Mail-Servern und Clients, S. 6.

SOCKS SOCKS ist eine Abkürzung für SOCKetS und ist ein Protokoll für einen Circuit Relay Proxy der im Gegensatz zum Proxy auf Anwendungsebene den Verbindungsaufbau für den Benutzer transparent realisiert[65], S. 10.

SSL Secure Socket Layer ist ein Verschlüsselungsprotokoll zur Datenübertragung und wird vor allem bei auf Webservern mit dem Protokoll HTTPS eingesetzt[30], S. 58.

SYN SYN ist ein Flag einer TCP-Verbindung und ist das erste was beim Verbindungsaufbau zwischen zwei Programmen gesendet wird[30], S. 7.

TCP Transmission Control Protocol zum verbindungsbehafteten Aufbau einer Verbindung zwischen zwei Programmen[30], S. 7.

UDP User Datagram Protocol zur Verbindungslosen Datenübertragung zwischen zwei Programmen[30], S. 7.

URL Der Uniform Resource Locator wird zum Identifizieren einer Ressource im Netzwerk verwendet. Er kann aus der Angabe eines Protokolls, einer Authentifizierung, einem Host mit Port, einem Pfad, einer Query und einem Anker bestehen, S. 6.

Literaturverzeichnis

[1] Daniel Bachfeld. Sql-injection - angriff und abwehr. http://www.heise.de/security/Giftspritze--/artikel/43175/0.

[2] James Eaton-Lee Barrie Dempster. *Configuring IPCop Firewalls - Closing Borders with Open Source*. Packt Publishing, 1 edition, September 2006.

[3] Cord Beermann. Calamaris. http://cord.de/tools/squid/calamaris/.

[4] Tim Berners-Lee. Information management: A proposal. http://www.w3.org/History/1989/proposal.html.

[5] Übersetzer: ansuess Ceelight Daniel S. Mäuschen30 zisoft. *IPCop-Installationshandbuch*, 1 edition, 2005. http://www.ipcop-forum.de/manuals/other/ipcop-install-de-1.4.x.pdf.

[6] Übersetzer: Christian Werner-Meier dotzball enricoballa Fast.Edi Dirk Linnenfelser. *IPCop-Administrationshandbuch*, 1 edition, 2006. http://www.ipcop-forum.de/manuals/other/ipcop-admin-de-1.4.x.pdf.

[7] Bitkom. Private computernutzung steigt in deutschland auf 70 prozent. http://www.bitkom.org/de/presse/30739_49655.aspx.

[8] Jérémy Chartier. About snortalog. http://jeremy.chartier.free.fr/snortalog/.

[9] R. Droms. Dynamic host configuration protocol. http://tools.ietf.org/html/rfc2131.

[10] R. Droms. Glossary of spam terms. http://www.sophos.com/security/spam-glossary.html.

[11] R. Droms. The mime multipart/related content-type. http://tools.ietf.org/html/rfc2387.

[12] Tom Eichstaedt. Ipcop v1.4.x | sysinfo gui addon. http://www.ipadd.de/binary.html.

[13] Stephan Feddersen. Guiports. http://www.h-loit.de/index.php?option=com_content&task=view&id=28&Itemid=51.

[14] Stephan Feddersen. Installation des guiports addon. http://www.h-loit.de/index.php?option=com_content&task=view&id=87&Itemid=87.

[15] Stephan Feddersen. Installation des linetest addons. http://www.h-loit.de/index.php?option=com_content&task=view&id=71&Itemid=77.

[16] Stephan Feddersen. Installation des ups server addons. http://www.h-loit.de/index.php?option=com_content&task=view&id=12&Itemid=41.

[17] Stephan Feddersen. Installation des webalizer xtended addons. http://www.h-loit.de/index.php?option=com_content&task=view&id=77&Itemid=82.

[18] Stephan Feddersen. Linetest. http://www.h-loit.de/index.php?option=com_content&task=view&id=27&Itemid=52.

[19] Stephan Feddersen. Ups server. http://www.h-loit.de/index.php?option=com_content&task=view&id=23&Itemid=40.

[20] Stephan Feddersen. Webalizer xtended. http://www.h-loit.de/index.php?option=com_content&task=view&id=26&Itemid=49.

[21] Eckart Gutzeit. Alles über vpns. http://ipcop.gutzeit.ch/tutorialsinfos/3-alles-uber-vpns/.

[22] Markus Hoffmann. High availability addon v2.3. http://mh-lantech.css-hamburg.de/ipcop/download.php?view.144.

[23] Markus Hoffmann. Rootkithunter 1.2.9. http://mh-lantech.css-hamburg.de/ipcop/download.php?view.169.

[24] Markus Hoffmann. Snortalog 2.40rc2 für ipcop. http://mh-lantech.css-hamburg.de/ipcop/download.php?view.113.

[25] Markus Hoffmann. Ucarp. http://mh-lantech.css-hamburg.de/ipcop/wiki/index.php?title=Ucarp.

[26] http://sourceforge.net/projects/rkhunter/. Rootkit hunter frequently asked questions (faq). http://sourceforge.net/docman/display_doc.php?docid=35179&group_id=155034.

[27] IPCop.org. Ipcop hardware compatibility list. http://www.ipcop.org/index.php?module=pnWikka&tag=IPCopHCLv01.

[28] Patrick McHardy Klaus Rechert. Hfsc scheduling mit linux, 2005. http://klaus.geekserver.net/hfsc/hfsc.html.

[29] Steve Kostecke. Welcome to the ntp.servers web. http://support.ntp.org/bin/view/Servers/WebHome.

[30] Andreas G. Lessig. *Linux-Firewalls - Ein praktischer Einstieg*. O'Reilly, 2 edition, Januar 2006.

[31] Markus Madlener. Copfilter - documentation. http://www.copfilter.org/docu.php.

[32] Markus Madlener. *Copfilter - An add-on for the IPCop Firewall*, 1 edition, 2005. http://members.inode.at/m.madlener/copfilter/README.pdf.

[33] Justin Mason. Spamassassin - what is spamassassin?, 2006. http://wiki.apache.org/spamassassin/SpamAssassin.

[34] Markus Hoffmann Michael Winkler. fwlogs 1.1.1 ipcop 1.4.11. http://mh-lantech.css-hamburg.de/ipcop/download.php?view.167.

[35] Robert Morris. Robert morris. http://pdos.csail.mit.edu/~rtm/.

[36] Besim Karadeniz Netplanet. Das phänomen world wide web. http://www.netplanet.org/geschichte/worldwideweb.shtml.

[37] Eric Oberlander. *Quick Start*, 1 edition, 2004. http://www.ipcop-forum.de/quickstart.php.

[38] Peter Siering. Xenisiert - c't debian-server 2 mit xen 3.1. *c't*, pages 133–137, Juni 2007.

[39] Marco Sondermann. Calamaris proxy report generator add-on. http://www.advproxy.net/calamaris/.

[40] Marco Sondermann. *updatexlrator - Update Accelerator Administrator's GUIde*, 1 edition, 2006. http://www.advproxy.net/update-accelerator/documentation/ipcop-updatexlrator-en.pdf.

[41] Marco Sondermann. *advproxy - Advanced Web Proxy Administratorhandbuch*, 1 edition, 2007. http://www.advproxy.net/documentation/ipcop-advproxy-de.pdf.

[42] Marco Sondermann. advproxy - frequently asked questions, 2007. http://www.advproxy.net/faq.html.

[43] Marco Sondermann. advproxy - the advanced web proxy add-on for ipcop and smoothwall, 2007. http://www.advproxy.net/.

[44] Marco Sondermann. calamaris - calamaris proxy report generator add-on, 2007. http://www.advproxy.net/calamaris/.

[45] Marco Sondermann. updatexlrator - update accelerator add-on for ipcop, 2007. http://www.advproxy.net/update-accelerator/.

[46] Marco Sondermann. updatexlrator - update accelerator add-on for ipcop, 2007. http://www.ipcopwiki.de/index.php/Axel#Eigene_Downloadquellen_integrieren.

[47] Marco Sondermann. Url filter faq overview, 2007. http://www.urlfilter.net/faq.html.

[48] Marco Sondermann. Url filter quick reference, 2007. http://www.urlfilter.net/quickreference.html.

[49] Marco Sondermann. urlfilter - the url filter add-on for ipcop and smoothwall, 2007. http://www.urlfilter.net/.

[50] Ralf Spenneberg. *Intrusion Detection für Linux-Server - Mit Open Source-Tools Angriffe erkennen und analysieren*. Markt + Technik, 1 edition, November 2002.

[51] Ralf Spenneberg. *Intrusion Detection und Prevention mit Snort 2 & Co. Einbrüche auf Linux-Servern erkennen und verhindern*. Addison-Wesley, 1 edition, November 2004.

[52] Ralf Spenneberg. *Linux Firewalls mit iptables & Co*. Addison-Wesley, 1 edition, Februar 2006.

[53] Endian S.r.l. Endian software edition. http://www.endian.com/en/products/firewall/software/.

[54] Arie Tal. Two technologies compared:nor vs. nand - white paper. http://www.data-io.com/pdf/NAND/MSystems/MSystems_NOR_vs_NAND.pdf.

[55] Achim Weber. Blockouttraffic (bot) for ipcop 1.4.x, 2006. http://blockouttraffic.de/index.php.

[56] Achim Weber. Bot - frequently asked questions, 2006. http://blockouttraffic.de/faq.php.

[57] Achim Weber. Bot - getting started, 2006. http://blockouttraffic.de/gettingstarted.php.

[58] Achim Weber. Bot - installation, 2006. http://blockouttraffic.de/installation.php.

[59] Olaf Westrik. Aktuelle coptime-statistik: Anzahl der mitglieder. http://www.ipcop-forum.de/coptime/members.php.

[60] Olaf Westrik. Aktuelle coptime-statistik: Durchschnittliche uptime. http://www.ipcop-forum.de/coptime/average.php.

[61] Olaf Westrik. Aktuelle coptime-statistik: Summe der uptimes. http://www.ipcop-forum.de/coptime/total.php.

[62] Olaf Westrik. Coptime addon/ipcop uptime client. http://www.ipcop-forum.de/forum/viewtopic.php?t=15344.

[63] www.IPCop forum.de. Ipcop und virtuelle maschinen. http://www.ipcop-forum.de/unipcop.php.

[64] www.IPCop.org. Ipcop roadmap. http://www.ipcop.org/index.php?module=pnWikka&tag=IPCopRoadmap.

[65] Robert Ziegler. *Linux Firewalls - Konzeption und Implementierung für kleine Netzwerke und PCs*. Markt und Technik, 2 edition, 2000.

[66] Mario Zimmermann. Modifiziertes mkflash für ipcop 1.4.x. http://www.zisoft.de/ipcop/mkflash/.

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ohne unerlaubte Hilfsmittel angefertigt worden ist, insbesondere dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche gekennzeichnet habe. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Weiterhin erkläre ich, dass die Arbeit in gleicher Form oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat. Ich erkläre mich damit einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird.

Nettetal, 14.02.2008

Stefan Kox